

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s)) Scott E. HRASTAR
Application No.) 10/700,914
Filing Date) November 4, 2003
Title) SYSTEMS AND METHODS FOR DETERMINING
WIRELESS NETWORK TOPOLOGY
Examiner) Backhean Tiv
Art Unit) 2151
Confirmation No.) 7780

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450 USA

DECLARATION UNDER 37 CFR § 1.131

Dear Madam or Sir,

I, Scott E. Hrastar, hereby declare that:

1. I am the inventor in Application No. 10/700,914, filed on November 4, 2003. Application No. 10/700,914 claims priority to U.S. Provisional Application No. 60/464,464 filed on April 21, 2003.
2. The attached Exhibit A is a true copy of an original document prepared in the regular course of business of AirDefense, Inc., the assignee of the above-identified application, and that the original is in the possession of AirDefense, Inc.
3. Exhibit A is an excerpt from the User Guide for AirDefense Release 3.0. Exhibit A was made in this country (U.S.A.) prior to the February 14, 2003 priority date of Williams *et al.* (U.S. Pat. Publication No. 2005/0015623), and the February 13,

2004 filing date of Williams *et al.* The corresponding dates of Exhibit A show a conception and reduction to practice of the present invention prior to the priority date and filing date of Williams *et al.* See, *e.g.*, page 1 of Exhibit A.

4. Exhibit A details functionality of the present invention. Specifically, pages 2 – 4 describe repeated monitoring of a wireless network to detect security and policy violations. Pages 5 – 60 describe a topology representation of the wireless network and detection of potential security and policy violations through a comparison of topology data.

I hereby declare that all statements made in this instrument of my knowledge are true and all statements made on information and belief are believed to be true and further that these statements are made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Respectfully submitted,

Date: 4/8/08

Scott E. Hrastar

Scott E. Hrastar

Copyright © [REDACTED] AirDefense, Inc. All rights reserved.
Printed in the United States of America

Proprietary Notices

AirDefense is licensed software and hardware. Its use is subject to the terms and conditions of a license agreement or nondisclosure agreement between AirDefense, Inc. and its customers. It is against the law to copy the software on any medium except as specifically allowed in the license or nondisclosure agreement.

Information contained in this document is subject to change. No part of this manual and/or software may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than personal use by AirDefense, Inc. without the express written permission of AirDefense, Inc.

Trademarks

AirDefense™ is a trademark of AirDefense, Inc. in the U.S. and other countries.
All other trademarks are the property of their respective owners.

Cautionary Statements

- **Caution:** There are no user-serviceable components inside the AirDefense Server appliance. Opening the chassis will void your service agreement.
- **Caution:** The recommended ambient operating temperature of the AirDefense Server appliance is 0°C—55°C. Installation in a closed or multi-rack assembly may raise the immediate ambient temperature above the average room temperature. Exercise due caution.
- **Caution:** Provide adequate spacing above, below, and behind the AirDefense Server appliance, to allow proper air flow, and to prevent excessive heat buildup.
- **Caution:** Use only industry-standard mounting kits when installing the AirDefense Server appliance, as improper mounting may result in hardware failure and hazardous conditions.
- **Caution:** Ensure that the electrical circuit through which the appliance is powered can safely accommodate the AirDefense Server's 300 Watt power supply.

Publication History

[REDACTED] Issue 1.00 of this document, for AirDefense software Release 2.0

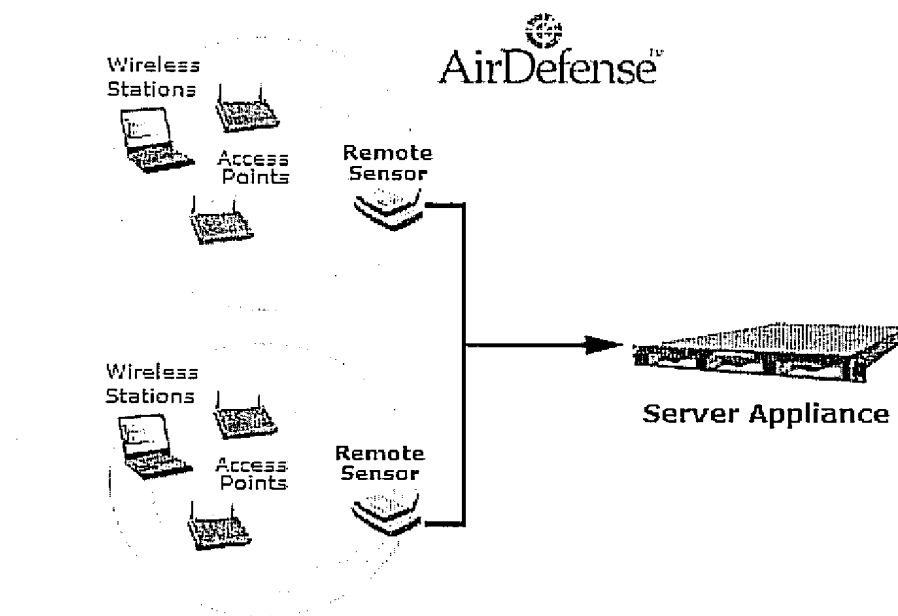
[REDACTED] Issue 1.01 of this document, for AirDefense software Release 2.1

[REDACTED] Issue 1.02 of this document, for AirDefense software Release 3.0

AirDefense is a WLAN intrusion protection and management system. It consists of three components: physical Sensors that are placed at strategic locations in your WLAN; a management appliance—the AirDefense Server—that receives information from the Sensors; and a management console that runs the AirDefense Server. AirDefense authorizes and monitors the traffic of every User Station (wireless-capable laptops and workstations) in your WLAN.

AirDefense does the following:

- Provides proactive WLAN defenses. AirDefense discovers network vulnerabilities and threats – such as rogue Access Points and ad hoc networks – as they happen.
- Detects intruders and attacks on the WLAN, and eliminates those threats.
- Provides robust WLAN management functions that allow you to understand your WLAN, monitor network performance, and enforce network policies.



2.1 The AirDefense Solution

The AirDefense solution consists of distributed Sensors and centrally managed Servers that reside near 802.11 Access Points.

- The AirDefense Server analyzes traffic in real time to detect intrusions, impending threats, and attacks.
- Sensors monitor all WLAN activities and report back to the AirDefense Server, which analyzes the traffic in real time. The Sensors provide 24x7 monitoring of WLAN traffic and activities. Sensors are centrally managed by the AirDefense Server.

With its combination of properly deployed Servers and Sensors, AirDefense enforces WLAN policies, monitors WLAN performance, helps network administrators troubleshoot network issues, and provides comprehensive reporting. AirDefense is configurable, so you can identify both authorized and unauthorized Stations and Access Points that are transmitting and receiving data within your network— even users on the perimeter of your wireless air space.

AirDefense is the only WLAN security solution that provides 24x7, real-time tracking of the airwaves. It monitors the state of every Access Point and Station transmitting on the airwaves and gives you a minute-by-minute account of all WLAN hardware statuses and wireless traffic. This enables you to immediately recognize intruders, quickly detect attacks, and take appropriate measures to secure the network. A patent-pending State-Analysis Engine enables AirDefense to track and control the flow of communication on any enterprise WLAN.

Multi-Dimensional Detection and State Analysis Engines

AirDefense built its patent-pending Multi-Dimensional Detection Engine as a WLAN intrusion detection system.

A traditional intrusion detection system (IDS) is plagued by false positives because they rely on a single detection technology—mostly attack signatures. AirDefense has developed its Multi-Dimensional Detection Engine as a comprehensive WLAN intrusion detection system that integrates multiple detection technologies. These technologies correlate data to recognize real threats and reduce false positives. The State-Analysis Engine coordinates inputs and the Multi-Dimensional Detection Engine analyzes threats to identify security breaches based on:

- Signature analysis
- Policy compliance
- Protocol assessment
- Statistically anomalous behavior

After Initial Tuning

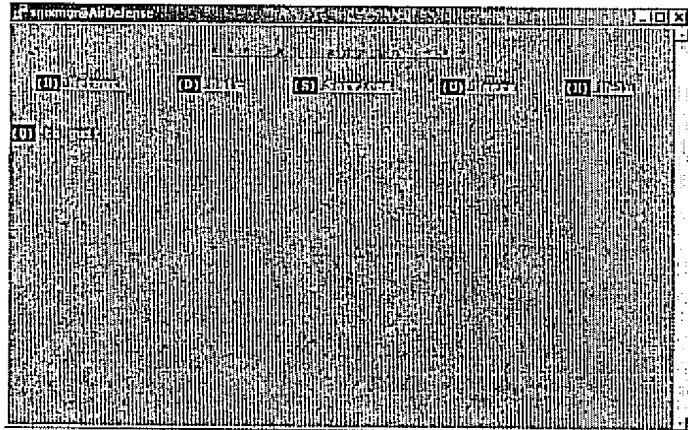
During the next few weeks you should monitor traffic patterns using AirDefense. During this time, AirDefense will record information about the devices in your WLAN, and the data those devices transmit and receive. The data is available via AirDefense Reports (see Chapter 7, Reports). After reviewing this information, retune the performance policy thresholds for Stations and Access Points (see "Create Policy: Performance" on page 103). To receive more accurate alarms, set threshold values that reflect your normal network traffic patterns. Now AirDefense will only generate Performance alarms when wireless activity falls outside the normal range of activity.

1.6 Setting AirDefense Time, Date, Time Zone, and NTP

You must use the Command Line Interface to set the time, date, time zone, and NTP (time synchronization with a network server). You set the time, date, time zone, and NTP via the Date program on the ADDadmin screen.

Note: If you are changing AirDefense time because, for example, you move the AirDefense Server's location from the east to west coast of the United States, you must also locate a *new* network time server in the same time zone.

Prerequisite: You should already be logged-in to the AirDefense Server, either locally or remotely, using the Command Line Interface (see "Logging On to the AirDefense Server" in this chapter). The ADDadmin screen must be in the terminal window.



Note: You may type any program command at the opening ADDadmin command prompt—it is not necessary to navigate first to the program page in order to execute a command within it. Whereas mis-typed commands in ADDadmin's secondary pages are forgiven, misspellings at the opening window log you out of the program.



5 Policy Manager

Policy Manager enables you to define policies and monitor your WLAN. Use Policy Manager to do the following:

- Create and apply policies for individual and multiple Sensors, Access Points, and Stations in your WLAN.
Policies are behaviors that you can assign to Sensors, Access Points, and Stations in AirDefense. When AirDefense detects traffic that violates your policies, it generates alarms and alarm reports.

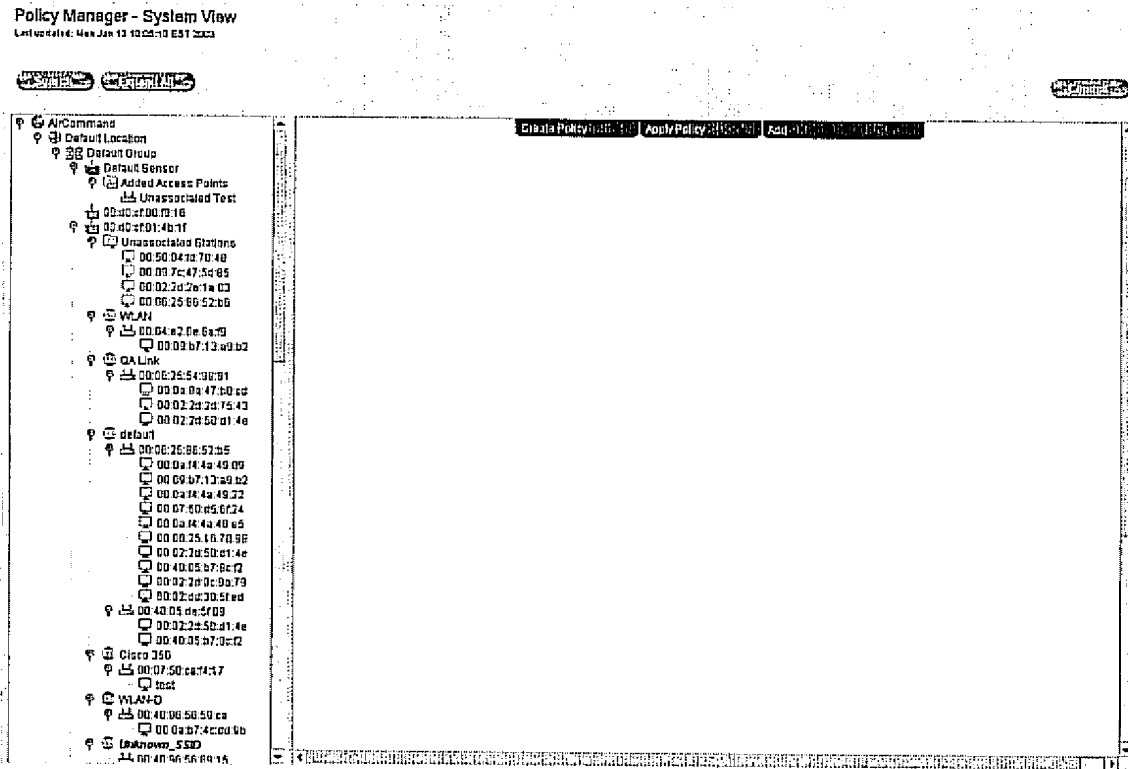
AirDefense has generic default policies designed for rapid deployment. AirDefense gives you the flexibility to go beyond the default policies by using Policy Manager's configuration editing function to form your own custom policies. Using the Policy Manager, you can create and apply your own alarm-generating policies to Sensors, Access Points, and Stations.
- Pre-configure and add Access Points and Stations into AirDefense, either manually, or by importing via flat file.
You can import lists of pre-authorized Access Points, Stations, and User Credentials from an ASCII comma delimited flat file.
- See views of the historical associations and behaviors of Sensors, Access Points, and Stations in your WLAN.
Using a icon and color-coded Tree View, Policy Manager gives you an historical observed state of the activity that has been taking place in AirDefense. You can use this information to track Access Point-Station associations so that you can better maintain your WLAN.

5.0.1 In This Chapter

This chapter contains the following topics.

Topic	Page
Navigating Policy Manager	79
Sensor Policy	91
AP View	94
Station View	96
Creating Policies	99
Applying Policies	115
Adding Access Points and Stations	123

The screen below shows the Policy Manager System View. It shows the working screen area on the right, and the Policy Manager Tree View on the left



5.1 Navigating Policy Manager

Policy Manager has two windows, the Policy Manager Tree View on the left, and the working screen on the right. The working screen has pull-downs that reveal more screens.

- To create and apply policies to individual Sensors, Access Points, and Stations, use the Tree View. See "Policy Manager Tree View" on page 79
- To create and apply policies to more than one Sensor, Access Point, and Station, use the pull-down menus. See "Using Policy Manager Screen Pull-Downs" on page 81

5.1.2 Policy Manager Tree View

The left-hand window is the Policy Manager Tree View—a hierarchical tree that uses color-coded icons to show the historical Location, Group, Sensor, SSID, Access Point, and Station associations in your WLAN network, and their state since last **Refresh**. The tree gives an historical, not real-time, view of states. It displays regardless of which Policy Manager configuration screen you are currently working in.

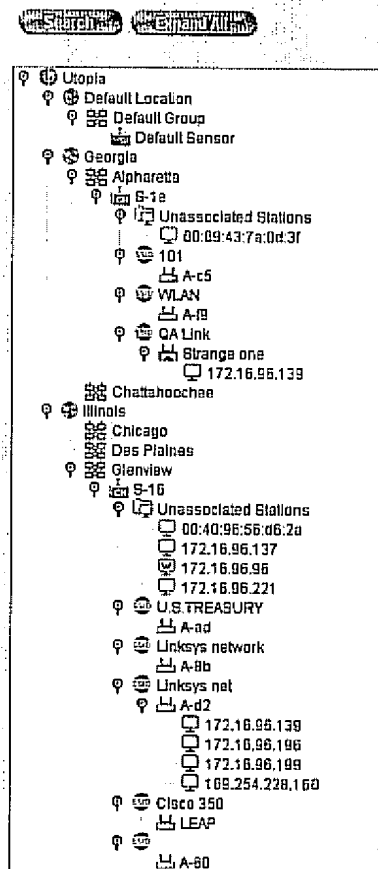
Tree View is navigational aide that will help you manage the Sensors, Access Points, and Stations in your WLAN. It is a true, structured hierarchy, with the highest level at AirDefense (system) View and the lowest level at Station View.

Each item in the tree has a color-coded icon that has a specific meaning (see "Color Codes" on page 83).

- **Colors** in Tree View identify the historical state of each network element on the tree (see "Color Codes" on page 83)
- **Icons** in Tree View identify network elements and their historical associations at the System, Location, Group, Sensor, Access Point, and Station levels (see "Icons" on page 86)
Important: In certain cases, the meanings of icons may differ slightly, depending on if the icon appears in the Tree View, or on one of the many screen tables that appear throughout the GUI. See "Icons" on page 86.

Policy Manager - System View

Last updated: Thu Dec 28 17:30:37 EST 2002



54.3 Using Policy Manager Tree View

Steps to Expand or Collapse Tree View

- 1 Click **Expand All** to expand Tree View.

The entire tree expands to display all Sensors, Access Points, and Stations in your network.



Note: Locations, Groups, Sensors, and Access Points appear only in one place on Tree View. Stations can appear in more than one place on Tree View, matching their associations with Access Points.

- 2 Click **Collapse All** to close the Tree View.

The entire tree collapses up to the System (your company) icon.



Steps to Update Tree View

You cannot move items around in Tree View. The tree is based on actual observed behaviors in the network. You can, however, delete Access Points and Stations from the tree. The AirDefense Server updates information as it receives new information, but the tree does not reflect these changes automatically. You cannot move items in the tree itself, as the tree is based on actual observed behaviors in the network. To keep track of the Sensor, Access Point, and Station associations in you network, you must manually update the tree.

Step	Action
------	--------

- | | |
|---|---|
| 1 | Click on Refresh at the top right corner of your screen. |
|---|---|

The tree will immediately reflect configuration changes made throughout the entire AirDefense GUI.



Configuring Individual Sensors, Access Points, and Stations

You can use Tree View to create and apply policies for **individual** Sensors, Access Points, and Stations in your WLAN. You can access three screens, which appear to the right of the tree, by clicking on icons directly on Tree View. These are:

- Sensor Policy (see "Sensor Policy" on page 91)
- AP View (see "AP View" on page 94)
- Station View (see "Station View" on page 96)

The table below describes the configuration screens.

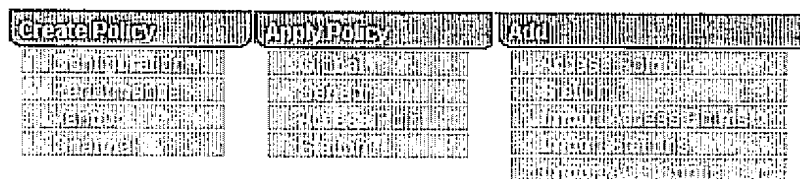
Field	Description
Sensor Policy	Access this field by clicking on a Sensor on Tree View. Use this field to set a Sensor's CRC Errors Threshold and to edit Channel Policies per Sensor.

Field	Description
AP View	<p>Access this field by clicking on an Access Point on Tree View.</p> <p>Use this field to view information about an Access Point. You can also use this field to enter an Access Point's name, designate the Access Point as a bridge, Authorize/Unauthorize/Ignore the Access Point, or edit the Access Point's Configuration, Performance, or Vendor policies.</p>
Station View	<p>Access this field by clicking on a Station on Tree View.</p> <p>Use this field to view Station information, including Access Point associations. You can also use this field to enter a Station name, a Station Description, a Station IP address, place the Station on a Watch List or Ignore List, and Authorize/Unauthorized Stations for Access Points.</p>

6.1.4 Using Policy Manager Screen Pull-Downs

The Policy Manager screen has pull-downs. Use these to create and apply policies for multiple Access Points and Stations, and to add Access Points and Stations to your WLAN. The pull-downs are:


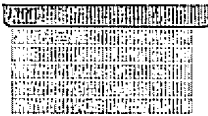
- Create Policy
- Apply Policy
- Add



The table below describes the pull-downs

Field	Description
Create Policy	<p>Access this set of AirDefense fields from the main Policy Manager screen. Use these fields to create configuration, performance, vendor, and channel policies for your Sensors, Access Points, and Stations. The screens are:</p> <ul style="list-style-type: none"> • Configuration • Performance • Vendor • Channel fields



Field	Description
Apply Policy	<p>Access this set of AirDefense fields from the main Policy Manager screen. Use these fields to apply Global, Access Point, Sensor, and Station policies to your Access Points, Sensors, and Stations. The screens are:</p> <ul style="list-style-type: none"> • Global • Sensor • Access Point • Station 
Add	<p>Access this set of AirDefense fields from the main Policy Manager screen. Use these fields to pre-configure (including authorization) and add Access Points or Stations to your network, import Access Points or Stations from another location, and add ACS Configurations to your WLAN. The screens are:</p> <ul style="list-style-type: none"> • Access Point • Station • Import Access Points • Import Stations • Add ACS Configuration. 

5.1.5 Color Codes

Each icon that appears in Policy Manager in either the Tree View or the GUI screens has a color that represents a state.

- Individual Access Points and Sensors display in a single color that represents their current state.
- A single Station can display in two or more colors, depending on its configuration in relationship to its Access Point.

Important: In certain cases, the meanings of icons may differ slightly, depending on if the icon appears in the Tree View, or on one of the many screen tables that appear throughout the GUI.

The table below lists the colors and their meanings.

Color	Meaning
Blue	<p>Blue indicates a default placeholder state for Sensors, Access Points, or Stations that are not observed by AirDefense. Placeholder items are always a manually-added or an imported Access Point or Station. They will always be Blue.</p> <p><i>Note:</i> When you import an Access Point that has never been entered into AirDefense, it will be Blue, even if you authorized in its configuration in the import file. When AirDefense detects the newly imported Access Point, the state changes to either authorized (Green) or unauthorized (Red), depending on your configuration in the import file.</p>
Grey	<p>Grey indicates that a Access Point or Station is being ignored by the AirDefense Server. For more information on Ignore, see Chapter 5, Policy Manager.</p> <p><i>Note:</i> AirDefense sees devices that are in the ignored state, but does not generate an alarm unless an attack occurs.</p>

Color	Meaning
Red	<p>Red indicates the following:</p> <ul style="list-style-type: none"> • Sensor: Offline, which indicates that the Sensor is not communicating with the AirDefense Server for one of the following reasons: <ul style="list-style-type: none"> — Sensor has been observed by the Server, but is currently not connected to the Server. — Sensor is connected to the Server, but is configured for Active: no operation (see "Configuring Sensors" on page 19). <p><i>Note:</i> If you did not intentionally take a Sensor offline, perform appropriate steps to reboot the Sensor (see Chapter 1, Installation & Log In).</p> • Access Point: Unauthorized <ul style="list-style-type: none"> — All Access Points are unauthorized when they are first discovered by AirDefense. They remain unauthorized until an administrator changes their state to authorized. If you manually add or import an Access Point, you can configure it as authorized at that time, in which case, it enters AirDefense as Blue. • Station: Unauthorized on a given Access Point <ul style="list-style-type: none"> — Unauthorized indicates that the Station is not authorized for the Access Point it appears under — The same Station can appear as Red or Green, depending on whether or not they are authorized on the Access Point they are under — Stations have a W on Green or Red if they are on the user-configurable Watch List (for more information on the Watch List, see Chapter 5, Policy Manager). <p><i>Note:</i> AirDefense generates an alarm once per minute, per device, as long as the device remains unauthorized.</p>
Green	<ul style="list-style-type: none"> • Stations <ul style="list-style-type: none"> — Station is authorized under the Access Point and has been observed as associated to that Access Point • Access Points <ul style="list-style-type: none"> — Access Point is authorized and has been observed by a Sensor • Sensor <ul style="list-style-type: none"> — Green indicates that the Sensor is functioning normally and in communication with the AirDefense Server. To be in this state, the following is required: <ul style="list-style-type: none"> >>The Sensor must be connected to the Server—the Sensor IP address must match the Server IP address (see "Configuring Sensors" on page 19). >>The Sensor must be configured for Active: yes operation (see "Configuring Sensors" on page 19).


Color	Meaning
Purple	<p>Purple can have two meanings:</p> <ul style="list-style-type: none"> • In all GUI program areas with the exception of Policy Manager, Purple indicates that the Station has been observed, but not currently associated, with any Access Point at that time. • In Policy Manager, Purple indicates that a Station has never been associated with an Access Point.
Orange	<p>Orange indicates Ad Hoc activity. There are two Orange icons:</p> <ul style="list-style-type: none"> • Ad hoc Network • Ad hoc Station

6.16 Icons


Each network element in the AirDefense WLAN is represented by an icon. Icons can either represent a physical device, such as an Access Point, Station, or Sensor, or logical associations, such as an SSID, a Location, or a Group.

The tables below list the icons and their meaning


Magnifying Glass

Icon	Color/State	Meaning
	Static	<p>Magnifying Glass.</p> <p>This icon can appear on all items in the Tree View with the exception of the Station. It indicates that the item is expandable or collapsible. Clicking on the icon next to a tree item expands that item; clicking again, collapses the item.</p> <p>For example, clicking on the magnifying glass next to an Access Point reveals the Stations that have associated with that Access Point.</p>


AirDefense (System) Icon

Icon	Color/State	Meaning
	Static	<p>This is the highest level in the tree, representing the AirDefense Server.</p>

Location Icon




Icon	Color/State	Meaning
	Static	<p>This is the second highest level in the tree, representing the Sensor Location. Expand the Locations to expose the individual Groups for a particular Location.</p>

Group Icon


Icon	Color/State	Meaning
	Static	<p>This is the third highest level in the tree, representing the Sensor Group. Expand the Groups to expose the individual Sensors for a particular Group.</p>

Sensor Icons

Sensors can be three different colors, representing three states. These are Blue, Red, and Green. Sensor icons can also have a CH or SC on the icon. The CH indicates that the Sensor is configured for Channel Lock; the SC indicates that the Sensor is configured for Scan Channels (see "Configuring Sensors" on page 70 for more information on these configurations).










Icon	Color/State	Meaning
	Blue: Not observed by the AirDefense Server; not online or active	Default Sensor The Default Sensor is a placeholder, not a real online Sensor. This is a place to put Stations and Access Points that you have manually added or imported, and authorized into AirDefense. AirDefense has not yet physically observed these. <i>Note:</i> Access Points entered into AirDefense always appear as blue, and always at the top of the tree under Default Sensor until they are seen by AirDefense. Once observed, they become green, red, or grey, and are moved out of the list, but not automatically. You must click Refresh .
	Green: Online CH =Channel Lock SC =Channel Scan	Online Sensor Sensor is functioning normally and is communicating with the AirDefense Server. To be in this state, the following are required: <ul style="list-style-type: none"> The Sensor must be connected to the Server—the Sensor IP address must match the Server IP address (see "Configuring Sensors" on page 19). The Sensor must be configured for Active: yes operation (see "Configuring Sensors" on page 19).
	Red: Offline CH =Channel Lock SC =Channel Scan	Offline Sensor Sensor is not communicating with the AirDefense Server for one of the following reasons: <ul style="list-style-type: none"> Sensor has been observed by the Server, but is currently not connected to the Server. Sensor is connected to the Server, but is configured for Active: no operation (see "Configuring Sensors" on page 19).

SSID Icon

Icon	Color/State	Meaning
	Static	SSID This is the logical group to which the Access Points belong.

Access Point Icons








Access Points and Bridged Access Points can be four different colors, representing four states. These are Blue, Red, Green, and Grey.



Icon	Color/State	Meaning
	Blue: Unobserved	Unobserved Access Point Access Points that are blue are not yet seen by a Sensor.
	Blue: Added Access Point Folder	Added Access Point Folder This folder contains Access Points that have been added manually or imported, but have not yet been seen by a Sensor.
	Green: Authorized	Authorized Access Point <i>Note:</i> Access Points that you enter manually or import appear as blue, and always at the top of the tree under Default Sensor. Once they are seen by AirDefense, they are moved out of the list, but not automatically. You must click Refresh .
	Red: Unauthorized	Unauthorized Access Point On discovery, all Access Points come into AirDefense unauthorized. <i>Note:</i> An exception to this is if you previously added or imported the Access Point, at which time you can choose to authorize the Access Point. When it is seen by AirDefense, the Access Point will change from blue to green and move under the discovering Sensor.
	Grey: Ignored	Ignored Access Point Sensors can detect Access Points in neighboring WLAN systems. When this happens, AirDefense generates alarms. Designating an Access Point as Ignored prevents the Access Point and all Stations associated with the Access Point from alarming. If an attack occurs, an alarm generates regardless.
   	Blue: Unobserved Green: Authorized Red: Unauthorized Grey: Ignored	Bridged Access Point <i>Note:</i> Bridges are user-defined for informational purposes. Two or more Access Points can serve as bridges to the wired network. Unlike regular Access Points, bridges do not have an Ethernet connection to the physical network. They are configured to transmit data they receive to a specific Access Point—either another bridge or to a wired Access Point. For more information, see Appendix D on page 259.

Station Icons


Stations can be five different colors, representing five states. These are Purple, Green, Red, Grey, and Orange.

- Green and Red Stations can have a "W" on the icon, indicating they are on the Watch List.
- A Station can appear as Green, Red, or Grey under different Access Points, depending on the configuration.

Icon	Color/State	Meaning
 	<p>Purple: Unassociated</p> <p>Purple with "W": Authorized, and on Watch List</p>	<p>Unassociated Station</p> <p>Purple Stations have two meanings:</p> <ul style="list-style-type: none"> • In all GUI program areas with the exception of Policy Manager, a Purple Station indicates that the Station has been observed, but not currently associated with any Access Point at that time. • In Policy Manager, a Purple Station indicates that the Station has never been associated with an Access Point. It always appears under the Unassociated Stations folder in Policy Manager.
 	<p>Green: Authorized</p> <p>Green with W: Authorized, and on Watch List</p>	<p>Authorized Station</p> <p>This is a Station that is authorized on the Access Point it appears under. A W indicates that the Station is on the Watch List.</p> <p><i>Note:</i> An authorized Station may appear as Unauthorized (Red) or Ignored (Grey) under a different Access Point.</p>
 	<p>Red: Unauthorized.</p> <p>Red with W: Unauthorized, and on Watch List</p>	<p>Unauthorized Station</p> <p>This is a Station that is not authorized on the Access Point it appears under. A W indicates that the Station is on the Watch List.</p> <p>Unauthorized Stations generate alarms once per minute, per MAC address, for as long as the AirDefense Server recognizes the Station.</p> <p><i>Note:</i> An unauthorized Station may appear as Authorized (Green) or Ignored (Grey) under a different Access Point.</p>
	<p>Grey: Ignored</p>	<p>There are two types of Grey Stations:</p> <ul style="list-style-type: none"> • Station is configured for Ignore—<i>not alarm generating</i> <ul style="list-style-type: none"> — All activity by this Station is ignored by AirDefense. It does not generate alarms in AirDefense, regardless of activity. • Access Point is configured for Ignore—<i>alarm generating</i>. <ul style="list-style-type: none"> — If you configure an Access Point as Ignored, any Station under the Access Point also become Ignored in terms of traffic on that Access Point. If the Station starts doing anything outside of configured policies, AirDefense generates alarms.

Icon	Color/State	Meaning
	Orange: Ad Hoc;	<p>Ad Hoc Station</p> <p>An ad hocStation is a User Station that is connected to one or more other User Stations without using an Access Point. It does not need a wireless infrastructure, and therefore represents a security threat, especially when one or more User Stations in the ad hoc network also connect to a wired network. AirDefense detects ad hoc networks and reports the network's Device Identifiers and other information.</p>
	Grey folder/Blue Station: Unassociated	<p>Unassociated Stations</p> <p>The Unassociated Station folder contains Stations in a manual state that are observed by the AirDefense, but that have never been associated with an Access Point.</p> <p>Stations under this folder appear as Purple.</p>

Ad Hoc Network Icon

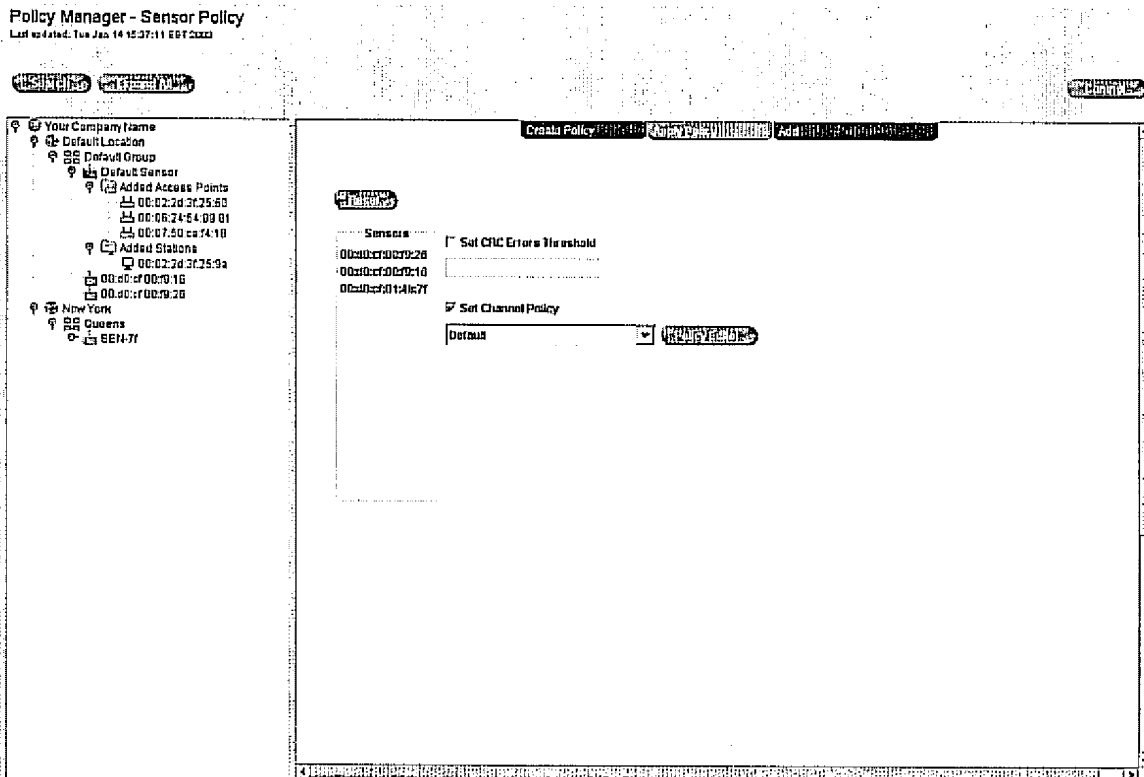
Icon	Color/State	Meaning
	Orange: Ad Hoc	<p>Ad Hoc Network</p> <p>An ad hoc network is a User Station that is connected to one or more other User Stations without using an Access Point. It does not need a wireless infrastructure, and therefore represents a security threat, especially when one or more User Stations in the ad hoc network also connect to a wired network. AirDefense detects ad hoc networks and reports the network's Device Identifiers and other information.</p> <p><i>Note:</i> The software that controls the functionality of wireless network adapters typically provides the ability, configured manually, to accomplish ad hoc networking. The software creates a session ID—much like the MAC address of an Access Point—which the devices use to communicate with each other.</p>

5.2 Sensor Policy

Use the **Sensor Policy** screen to configure CRC Errors Thresholds and Channel Policies for individual Sensors.

You can navigate to this screen by:

- Clicking on any individual Sensor in Tree View.

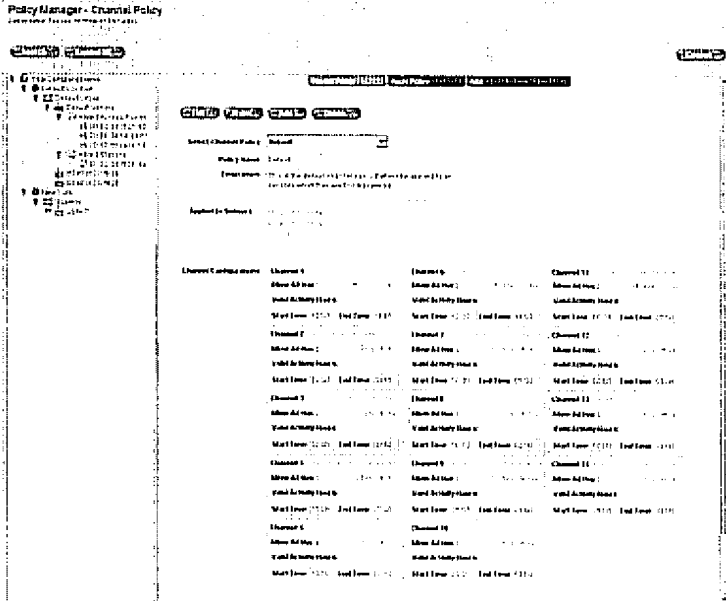


Steps to Use Sensor Policy

- | Step | Action |
|------|--|
| 1 | Click Expand All to expand Tree View and reveal the individual Sensors in the WLAN. |
| 2 | Click on any Sensor in Tree View to configure policies for an individual Sensor.
<i>The Sensor Policy screen appears.</i> |
| 3 | Configure CRC Errors Thresholds and Channel Policies for the individual Sensor. You must check the boxes to activate the fields. |
| 4 | Click Commit . |
| 5 | Alternately, you can click Reset to clear changes. |

The table below lists the fields in Sensor Policy.

Field	Purpose
Sensor ID	Device identifier of the Sensor.
Sensor Name	User-Configured Name of the Sensor. You designate the name of the Sensor when you configure the Sensor (see "Configuring Locations, Groups, and Sensors" on page 67). Example: <i>Floor One South.</i>
CRC Errors Threshold	This is the threshold for the number of CRC (transmission) errors allowed in the WLAN the Sensor is monitoring. Enter a number of CRC errors per minute each Sensor may detect as it listens to the traffic in its reception area. High numbers of CRC errors may indicate that two or more Access Points are sharing the same channel; colliding with each other; that an object is interfering with the signal; or that a hacker may be flooding your air space with bad data in a Denial of Service attempt. <i>Note:</i> Unusually high numbers of CRC errors indicate network performance problems or the activity of a hacker.

Field	Purpose
Channel Policy	<p>The pick list displays all saved channel policies. Select a channel policy from this list to apply to the Sensor. Default policies cannot be edited.</p> <p><i>Note:</i> Alternately, you can click Policy Editor to go to the Channel Policy Editor screen and edit, add, or delete channel policies for the Sensor (see "Create Policy: Channel" on page 112).</p>  <ul style="list-style-type: none"> • Channel Number: You must make configurations for each of the 14 channels. • Allow Ad Hoc: Choose Yes to allow Ad Hoc; No to disallow Ad Hoc. Ad Hoc is independent of activity hours <ul style="list-style-type: none"> <i>Note:</i> An ad hoc station is a User Station that is connected to one or more other User Stations without using an Access Point. Ad hoc networking is a function of most standard 802.11 network client cards. User Stations that are connected in this manner do not need a wireless infrastructure, and therefore represent a security threat, especially when one or more User Stations in the ad hoc network also connect to a wired network. • Valid Activity Hours: For each channel, enter a Start Time and End Time in the input fields. <ul style="list-style-type: none"> <i>Note:</i> Enter times in a 24-hour format, using the format HH:MM. Traffic is <i>only</i> allowed between the start and end hours. Traffic detected on the channel outside the valid activity hours generates an alarm.

Use the **AP View** screen to configure individual Access Points in your WLAN.

You can navigate to this screen by:

- Clicking on any individual Access Point in Tree View.

Policy Manager - AP View
Last updated: Thu Jun 23 10:10:00 EST 2011

Tree View:

- AirDefense
 - Default Location
 - Default Group
 - Default Sensor
 - Added Access Points
 - First Floor North
 - CA Link
 - 00:00:25:54:00:01
 - 00:00:00:00:00:00
 - 00:00:00:00:00:00




Configuration Fields:

Access Point ID: 00:07:d3:0e:6a:d9
 Access Point Name: First Floor North
 Description:
 Service Set ID:
 Access Point Vendor: Shark Digital Imaging B.V.
 IP Address:
 DNS Name:
 Bridge: ☐ Yes ☒ No
 Authorized Access Point: ☒ Yes ☐ No ☐ Ignore
 Configuration Policy: Default
 Performance Policy: Default
 Vendor Policy: Default

Steps to Use AP View

- | Step | Action |
|------|--|
| 1 | Expand Tree View reveals the individual Access Points in the WLAN. |
| 2 | Click on any Access Point in Tree View to configure policies for an individual Access Point.
<i>The AP View screen appears.</i> |
| 3 | Configure the fields in the screen. |
| 4 | Click Commit . |
| 5 | Alternately, you can click Reset to clear changes. |

The table below lists the fields.

| Field | Purpose |
|-------------------------|--|
| Access Point ID | Device Identifier of the Access Point. This is a required field. |
| Name | Name of the Access Point (optional). If you chose a name for the Access Point, it appears here. |
| Description | A description of the Access Point (optional) |
| Service Set ID | SSID number (this is not the same as the Access Point ID). |
| Access Point Vendor | Equipment manufacturer of the Access Point. This is automatically pulled by AirDefense. |
| IP Address | The IP address of the Access Point. |
| DNS Name | The Access Point's DNS Name assignment (if applicable). |
| Bridge | <ul style="list-style-type: none"> Yes: Click Yes if you are using this Access Point as a Bridge No: Click No if you are not using this Access Point as a Bridge <p><i>Note:</i> A Bridge is two or more Access Points that serve as bridges to the wired network. Unlike regular Access Points, bridges do not have an Ethernet connection to the physical network. They are configured to transmit data they receive to a specific Access Point—either another bridge or to a wired AP (see Appendix D: Glossary).</p> |
| Authorized Access Point | <ul style="list-style-type: none"> Yes: Click Yes to authorize this Access Point for use in your WLAN No: Click No to unauthorize this Access Point for use in your WLAN Ignore: Click Ignore to place this Access Point in an Ignored state. <p><i>Note:</i> Sensors can detect Access Points in neighboring WLAN systems. When this happens, AirDefense generates an alarm. Designating an Access Point as Ignored prevents the Access Point and all Stations associated with the Access Point from alarming. If an attack occurs, an alarm generates regardless.</p> |
| Configuration Policy | <p>Leave the default configuration policy for the Access Point in place, or specify a custom policy.</p> <p>Click Policy Editor to go to the Configuration Policy Editor screen if you wish to edit, add, or delete configuration policies.</p>  |
| Performance Policy | <p>Leave the default performance policy for the Access Point in place, or specify a custom policy.</p> <p>Click Policy Editor to go to the Performance Policy Editor screen if you wish to edit, add, or delete performance policies.</p>  |
| Vendor Policy | <p>Leave the default vendor policy for the Access Point in place, or specify a custom policy.</p> <p>Click Policy Editor to go to the Vendor Policy Editor screen if you wish to edit, add, or delete vendor policies.</p>  |

5.4 Station View

Use the **Station View** screen to configure individual Stations in your WLAN.

You can navigate to this screen by:

- Clicking on any individual Station in Tree View.

Policy Manager - Station View
Last updated: Tue Jan 14 15:52:29 EST 2003

Tree View:

- Your Company Name
 - Default Location
 - Default Group
 - Default Sensor
 - Added Access Points
 - 00:02:2d:3f:25:8a
 - 00:06:24:54:99:01
 - 00:07:50:ca:f4:18
 - Added Stations
 - 00:02:2d:3f:25:8a
 - 00:03:cf:00:00:16
 - 00:03:cf:00:00:26
- New York
 - Queens
 - SEI-IT

Main Configuration Area:

Station ID: 00:02:2d:3f:25:8a
Station Name: Station Zebra
Description: This is my station

LEAP Username:
Vendor Name: Agere Systems
IP Address: 172.16.96.131
DNS Name: airdefense.net
List Options: ☐ Watch List ☐ Ignore List

Access Points:
00:0e:25:54:99:01

☒ Set Authorization for Station on Access Points
☒ Authorized ☐ Unauthorized

Steps to Use Station View

- | Step | Action |
|------|---|
| 1 | Expand Tree View reveals the individual Stations in the WLAN. |
| 2 | Click on any Station in Tree View to configure policies for an individual Station.
<i>The Station View screen appears.</i> |
| 3 | Configure the fields in the screen. |
| 4 | Click Commit . |
| 5 | Alternately, you can click Reset to clear changes. |

The table below describes the fields in Station View.

| Field | Purpose |
|---------------|--|
| Station ID | MAC address of the Station. AirDefense automatically generates this field.
<i>Note:</i> You enter the Station ID when you add the Station to the WLAN (see "Add: Station" on page 126) |
| Name | User-configured name of the Station (optional).
<i>Note:</i> You can choose to give the Station a unique name, no longer than 15 characters, when you add the Station to the WLAN (see "Add: Station" on page 126). |
| Description | A description of the Station (optional).
<i>Note:</i> You can choose to give the Station a description when you add the Station to the WLAN (see "Add: Station" on page 126). |
| LEAP Username | This field applies if you are using EAP Configuration Mode in your configuration policy definition. (See "Create Policy: Configuration" on page 99.) |
| Vendor Name | Equipment manufacturer of the Station. AirDefense automatically generates this field. |
| IP Address | The IP address of the Station. This field displays an IP address if you chose to enter an IP address when you added the Station to the WLAN (see "Add: Station" on page 126). |
| DNS Name | The Station's DNS Name assignment (if applicable). |
| List Options | <p>If you are going to use a List Option, the option must be either Watch List, or Ignore.</p> <ul style="list-style-type: none"> • Watch List: Click on this checkbox if you wish to know if this Station's MAC address will occur in your network again. The next time the AirDefense Server sees this Station, it will generate an alarm for every minute the it sees this Station's in the network. • Ignore List: Click on this checkbox if you wish the AirDefense Server to ignore the presence of a Station on the network. AirDefense does not generate an alarm for any MAC address on the Ignore list. <p><i>Note:</i> This feature is useful if you want to keep certain unauthorized Stations that your AirDefense Server sees from alarming, as in the case of Stations in an adjacent office that belong to another Company. Placing these known "friendly" Stations on the Ignore list prevents continuous false alarms.</p> |

| Field | Purpose |
|--|---|
| Access Points | List of Access Points that the Station is associated with on your WLAN. Air-Defense pulls this list. |
| Set Authorization For Station on Access Points | <ul style="list-style-type: none"> You must click on the checkbox before selecting authorize/unauthorize. Authorize: Select Authorize if this Station is a legitimate Station assigned to an legitimate Access Point in your WLAN. Unauthorize: Select Unauthorize if this Station is not legitimate. If it is not authorized here, the AirDefense Server will generate an alarm once a minute whenever a Sensor detects the Station. (All detected Stations <i>not authorized</i> are assumed to belong to hackers or violators of your wireless network policy.) |



To create policies, you must access four screens. These are:

- Configuration
- Performance
- Vendor
- Channel

5.5.1 Create Policy: Configuration

Use the **Create Policy: Configuration** screen to create and edit configuration policies for multiple Access Points in your WLAN.

You can navigate to this screen by:

- Using the screen pull-down **Create Policy: Configuration**
- Clicking on any Access Point in Tree View, and then clicking **Configuration Policy: Policy Editor**.
- Clicking on **Apply Policy: Access Point**
- Clicking on **Ad Policy: Access Point**



Policy Manager - Configuration Policy
Last updated: Mon Jan 13 14:23:03 EST 2008

CONFIGURATION **PERFORMANCE** **VENDOR** **CHANNEL**

Tree View:

- AirCommand
 - Default Location
 - Default Group
 - Default Sensor
 - Added Access Points
 - Unassociated Test
 - 00:00:00:00:00:00
 - 00:00:00:00:00:00
 - Unassociated Stations
 - WLAN
 - QALink
 - default
 - Clisco 350
 - WLAN-D
 - Unknown_SSID
 - WLAN-B
 - wlan-a
 - fe:ed:00:00:00:00
 - fe:ed:01:00:00:00
 - fe:ed:02:00:00:00
 - fe:ed:03:00:00:00
 - fe:ed:04:00:00:00
 - BEH-71

Select Configuration Policy: Default

Policy Name: Default

Description:

Applied to Access Points:

- 00:00:00:00:00:00
- 00:00:00:00:00:00
- 00:00:00:00:00:00
- 00:00:00:00:00:00
- Unassociated Test
- Test

Authentication Modes: ☐ Open ☐ Shared Key ☒ LEAP ☒ 802.1x ☐ Other

Allowed WEP Modes: ☐ Off ☒ On ☐ Both

Allow SSID In Beacon: ☐ Yes ☒ No

Allowed Rates: ☒ 1 Mbps ☒ 2 Mbps ☒ 5.5 Mbps ☒ 11 Mbps

Fixed Channel: None

Steps to Use Create Policy: Configuration

- | Step | Action |
|------|--|
| 1 | Select the AirDefense (top) level of Tree View. |
| 2 | Click and pull down Create Policy: Configuration
<i>The Configuration Policy screen appears.</i> |
| 3 | To edit the fields, click on Edit .
<i>You can click Reset at any time to get out of Edit mode without saving your changes.</i> |
| 4 | To add a configuration policy to the database, click Add (Add is disabled while in Edit mode). |
| 5 | To permanently remove a configuration policy from the database, click Delete (Delete is disabled while in Edit mode). |
| 6 | Click Commit . |

The table below describes the fields in the **Create Policy: Configuration** screen.

| Field | Purpose |
|-----------------------------|--|
| Select Configuration Policy | Select the configuration policy from the pull-down.
<i>Note: You cannot configure a default policy.</i> |
| Policy Name | Enter the name of the policy in this field. |
| Description | Enter a description of the policy in this field. |
| Applied to Access Points | You cannot edit this field. This field shows the Access Points that your policy applies to. It lists the device identifiers of all Access Points detected by AirDefense in the last thirty days. |

| Field | Purpose |
|------------------------|--|
| Authentication Modes | <p>Choose a mode to configure the Access Point to accept non-authenticated network connections, and/or shared key authentication. AirDefense generate alarms if it detects that the Access Point is allowing Stations to associate with it using a method not allowed here.</p> <ul style="list-style-type: none"> • Open: This type of authentication allows any Station to associate with it—the equivalent of no authentication. • Shared Key: This type of authentication requires an encrypted key authentication before the Access Point allows Stations to associate with it. Key-sharing exposes the key to hackers. You may want to use an alternate authentication method—<i>Other</i>. • LEAP: EAP Authentication Mode--This option gives AirDefense the ability to detect LEAP authentication. You can set Access Point configuration policies to require LEAP authentication. Failure of the Access Point to operate contrary to this policy generates an alarm. Using this in your policy definition ensures that LEAP is deployed and being used by both Access Points and Stations. If an Access Point or Station is misconfigured and not running LEAP, AirDefense generates an alarm for either instance. • 802.1x: EAP Authentication Mode—This option gives AirDefense the ability to detect 802.1x authentication. You can set Access Point configuration policies to require 802.1x authentication. Failure of the Access Point to operate contrary to this policy generates an alarm. Using this in your policy definition ensures that 802.1x is deployed and being used by both Access Points and Stations. If an Access Point or Station is misconfigured and not running 802.1x, AirDefense generates an alarm for either instance. • Other: An alternate means of your choosing. |
| Allowed WEP Modes | <p>As a minimal security measure, you should enable Wired Equivalent Privacy (WEP) on every Access Point</p> <ul style="list-style-type: none"> • On: Enables WEP for the Access Point • Off: Disables WEP for the Access Point • Both: Allows either On or OFF, and does not generate an alarm for either. <p><i>Note:</i> Set the WEP policy to On and the Access Point to Off to enable alarms. If AirDefense detects the Access Point using WEP differently than specified here, it generates an alarm.</p> |
| Allowed SSID in Beacon | <p>SSID (Service Set IDs) are not passwords. They are broadcast in a beacon.</p> <ul style="list-style-type: none"> • Yes: Access Point broadcasts SSID • No: Access Point does not broadcast SSID <p><i>Note:</i> By default, many Access Points are configured to broadcast their Service Set ID (SSID) within their beacons.</p> <p><i>Note:</i> Set the SSID policy to No and the Access Point to Broadcast to enable alarms. If AirDefense detects that the Access Point beacon differs from what is specified here, it generates an alarm.</p> |

| Field | Purpose |
|---------------|---|
| Allowed Rates | <p>Each Access Point is configured to transmit and receive data at specified rates. Select the transfer rates you want the Access Point to use.</p> <ul style="list-style-type: none"> ▪ 1.0 Mbs ▪ 2.0 Mbs ▪ 5.5 Mbs ▪ 11 Mbs <p>If AirDefense detects the Access Point transmitting or receiving data at a rate not specified here, it generates an alarm.</p> |
| Fixed Channel | <p>If you want the Access Point to transmit on a fixed channel, you can specify the channel it uses from the pull-down channel list.</p> <ul style="list-style-type: none"> ▪ None ▪ 1-14 <p>If AirDefense detects the Access Point transmitting or receiving data on a different channel than indicated here, it generates an alarm.</p> |

5.6.2 Create Policy: Performance

Use the **Create Policy: Performance** screen to create and edit policies for network performance. These consist of a main screen, and three subscreens for configuring Performance Thresholds.

Note: AirDefense, Inc. recommends that you monitor network traffic for as long as several weeks, to determine normal network throughput before setting threshold values.

You can navigate to this screen by:

- Using the screen pull-down **Create Policy: Performance**
- Clicking on any Access Point in Tree View, and then clicking on **Performance Policy: Policy Editor**.
- Clicking on **Apply Policy: Access Point**
- Clicking on **Add: Access Point**

Policy Editor

Policy Manager - Performance Policy

Last updated: Tue Jan 14 10:00:10 EST 2003

Steps to Use Create Policy: Performance

- | Step | Action |
|------|---|
| 1 | Select the AirDefense (top) level of Tree View. |
| 2 | Click and pull down Create Policy: Performance |

The Performance field appears.

*Three sets of Performance Thresholds occupy the main body of the **Create Policy: Performance** field: These represent aggregate Station thresholds, individual Station thresholds, and Access Point thresholds. You can navigate through these subfields by clicking on the named folder tabs.*

| Aggregate Station | Station | Access Point |
|-----------------------------------|-----------|--------------|
| Associations per Minute | 20 | |
| Associated Stations | 5 | |
| Bytes into AP from Wired Net | 5,000,000 | |
| Bytes from AP to Wired Net | 5,000,000 | |
| Bytes between Stations in AP | 5,000,000 | |
| Bytes from Wired Net to Wired Net | 1,000,000 | |
| Total Data Frames Seen | 10,000 | |
| Total Mgmt Frames Seen | 2,000 | |
| Total Ctrl Frames Seen | 1,000 | |

| Aggregate Station | Station | Access Point |
|---------------------------|-----------|--------------|
| Associations per Minute | 2 | |
| Bytes Transmitted | 5,000,000 | |
| Bytes Received | 5,000,000 | |
| Data Frames Transmitted | 10,000 | |
| Data Frames Received | 10,000 | |
| Mgmt Frames Transmitted | 1,000 | |
| Mgmt Frames Received | 1,000 | |
| Ctrl Frames Transmitted | 500 | |
| Ctrl Frames Received | 500 | |
| Fragment Frames Seen | 1 | |
| Decrypt Error Frames Seen | 1 | |

| Aggregate Station | Station | Access Point |
|---------------------------|-----------|--------------|
| Associations per Minute | 1 | |
| Bytes Transmitted | 9,000,000 | |
| Bytes Received | 9,000,000 | |
| Data Frames Transmitted | 900,000 | |
| Data Frames Received | 900,000 | |
| Mgmt Frames Transmitted | 2,000 | |
| Mgmt Frames Received | 2,000 | |
| Ctrl Frames Transmitted | 2,000 | |
| Ctrl Frames Received | 2,000 | |
| Fragment Frames Seen | 1 | |
| Decrypt Error Frames Seen | 1 | |

- 3 To edit the Description and various Performance Thresholds, click **Edit**.
*You can click **Reset** at any time to get out of Edit mode without saving your changes.*
Note: When entering numerical values in the fields: If you want a single digit in the field, select the text and enter the value. You cannot backspace over the last digit in the field.
- 4 To add a performance policy to the database, click **Add** (Add is disabled while in Edit mode).
- 5 To permanently remove a performance policy from the database, click **Delete** (Delete is disabled while in Edit mode).
- 6 Click **Commit**.

The table below lists the top fields in the in the **Create Policy: Performance** screen.

| Field | Purpose |
|---------------------------|--|
| Select Performance Policy | This pick list displays all saved policies. Select a policy from this list to edit or delete it. Included in the list is a Default policy (cannot be edited). Newly-discovered Access Points are assigned this policy. |
| Policy Name | This displays the name of the policy. |
| Description | This displays a description of the policy. |
| Applied to Access Points | This memo field displays all Access Points currently configured to use the currently selected policy. |



About Thresholds

AirDefense generates alarms if it detects network traffic that exceeds the thresholds you enter in the Performance Thresholds fields. For each Access Point or Station triggering an alarm, AirDefense generates the alarm once per minute for every minute the condition exists. This allows you to detect whenever WLAN traffic exceeds normal limits, and allows you to perform network capacity planning—identifying when and where the WLAN needs to be augmented. You can monitor network traffic on a per-user basis, allowing you to identify which users are consuming the most bandwidth.

Initially, administrators should set global unauthorized station alarm policies to **Disable** after authorizing all Access Points for the first time. They will then create a *no alarm* Access Point policy and set all default thresholds to **zero**. This is to prevent AirDefense from filling with alarms during the initial deployment. Thresholds can be raised after successful deployment of AirDefense. For complete instructions on this process, see the *Quick Start* guide that came with AirDefense (AD-QS-1.01).

Aggregate Station Thresholds

Aggregate Station Thresholds are the *combined* network characteristics for all Stations and traffic in the Access Point's Basic Service Set (BSS)—i.e., the *footprint* of the Access Point and the Stations associating with it.

Note: Entering a zero value as a threshold anywhere within **Create Policy: Performance** disables alarm-generation for that threshold.

Example: For example, if the Associations Per Minute threshold for Aggregate Stations is zero, AirDefense will not generate an alarm—even if 5,000 associations are made within one minute.

| Aggregate Station | Station | Access Point |
|-----------------------------------|-----------|--------------|
| Associations per Minute | 20 | |
| Associated Stations | 3 | |
| Bytes into AP from Wired Net | 9,000,000 | |
| Bytes from AP to Wired Net | 9,000,000 | |
| Bytes between Stations in AP | 9,000,000 | |
| Bytes from Wired Net to Wired Net | 1,000,000 | |
| Total Data Frames Seen | 10,000 | |
| Total Mgmt Frames Seen | 2,000 | |
| Total Ctrl Frames Seen | 1,000 | |

The table below lists the field values in the Aggregate Station table.

| Values | Description |
|---|--|
| Associations per Minute | <p>Enter the maximum number of associations <i>per minute</i> AirDefense will allow between the Access Point and all Stations combined.</p> <p><i>Note:</i> On the one hand, this number should be low—for example, $\frac{1}{20}$ the number of total Stations in the WLAN. Your Stations should associate with an Access Point once in the morning when employees log on at the beginning of the workday, and rarely after that. On the other hand, if the threshold value represents the actual number of Stations in the BSS, a useful alarm will be generated if the Access Point goes offline, forcing the Stations to re-associate with it. In no case should this value be greater than the actual number of Stations in the BSS.</p> <p><i>Note:</i> If the signal strength between the Station and the Access Point is very low, the Station may repeatedly lose connectivity and then reconnect, increasing the number of associations per minute.</p> |
| Associated Stations
(Concurrently) | <p>Enter the maximum number of Stations allowed to associate <i>at any one time</i> with this Access Point. This number should reflect your actual number of Stations. If AirDefense detects a greater number, an alarm is generated, assuming that the extra associations are made by hackers.</p> |
| <p>The values for all the thresholds immediately below should be based upon your "site survey"—what you learned was "normal" for your WLAN.</p> <p><i>Note:</i> Take special care when creating the "byte thresholds" that immediately follow. Several factors govern the values you enter for each.</p> <ul style="list-style-type: none"> • The transmission rate of the Access Point—how much data it can transmit—is the first consideration. If the transmission rate is only 1 megabit per second, the thresholds should be much lower than if the transmission rate is 11 megabits per second. • All four directions of traffic (wired to wired, wired to wireless, wireless to wired, and wireless to wireless) must add up to 100% or less of available bandwidth. Many administrators prefer to set the individual thresholds such that their combined value is 80% or less than available bandwidth. • When setting thresholds designed for capacity planning, the threshold (for all data combined) should be approximately 50% of available bandwidth—that is, 30 MB per minute for an 11 MB transfer rate, and 3 MB per minute for a 1 MB transfer rate. | |
| Bytes into Access Point from Wired Net | <p>Enter the maximum number of bytes of data per minute allowed into the BSS from the wired portion of your network. If AirDefense detects a greater number, it generates an alarm.</p> |
| Bytes from Access Point to Wired Net | <p>Enter the maximum number of bytes of data per minute allowed out of the BSS to a wired portion of your network. If AirDefense detects a greater number, it generates an alarm.</p> |
| Bytes between Stations in BSS | <p>Enter the maximum number of bytes of data per minute allowed to be transmitted within the BSS from all Stations. If AirDefense detects a greater number, it generates an alarm.</p> |
| Bytes from Wired Net to Wired Net | <p>Enter the maximum number of bytes of data per minute allowed to be transmitted from a wired portion of the network to another wired portion of the network, using the Access Point as a bridge. If AirDefense detects a greater number, it generates an alarm.</p> |

| Values | Description |
|------------------------|---|
| Total Data Frames Seen | Enter the maximum number of data frames per minute allowed to be transmitted from all Stations combined. If AirDefense detects a greater number, it generates an alarm. |
| Total Mgmt Frames Seen | Enter the maximum number of management frames per minute allowed to be transmitted from all Stations combined. If AirDefense detects a greater number, it generates an alarm. |
| Total Ctrl Frames Seen | Enter the maximum number of control frames per minute allowed to be transmitted from all Stations combined. If AirDefense detects a greater number, it generates an alarm. |

Individual Station Thresholds

This set of thresholds apply to any *individual* Station in the Access Point's Basic Service Set, and will typically be lower than the Aggregate Station thresholds. That is, if any *single* Station reaches one of these thresholds, an alarm will be generated. These threshold alarms will tell you *who* the high bandwidth users are, and *when* they are using it. Entering a value of "0" (zero) for any threshold-type disables that specific alarm.

| Aggregate Station | Station | Access Point |
|---------------------------|-----------|--------------|
| Associations per Minute | 2 | |
| Bytes Transmitted | 5,000,000 | |
| Bytes Received | 5,000,000 | |
| Data Frames Transmitted | 10,000 | |
| Data Frames Received | 10,000 | |
| Mgmt Frames Transmitted | 1,000 | |
| Mgmt Frames Received | 1,000 | |
| Ctrl Frames Transmitted | 500 | |
| Ctrl Frames Received | 500 | |
| Fragment Frames Seen | 1 | |
| Decrypt Error Frames Seen | 1 | |

| Column | Description |
|---|---|
| Associations per Minute | Enter the maximum number of associations per minute any Station is allowed to make with an Access Point. On the assumption that most Stations should only associate once when the user logs onto to the network at the start of each work day, and rarely re-associate after that, this number should be low—1 or 2. If AirDefense detects a greater number, it generates an alarm. |
| The thresholds below should either be based on the "normal" transmission rate that you detected during your initial "site survey," or on arbitrary numbers designed to detect your high-bandwidth users. If you want to be notified, for example, of users who transmit files greater than 10 MB set the "Bytes Transmitted" and "Bytes Received" values to 10,000. If you don't care if users send large files, then set these values to zero (indicating that an alarm for that threshold will not be generated). | |

| Column | Description |
|---------------------------|--|
| Bytes Transmitted | Enter the maximum number of bytes of data per minute any Station is allowed transmit. If AirDefense detects a greater number, it generates an alarm. |
| Bytes Received | Enter the maximum number of bytes of data per minute any Station is allowed to receive. If AirDefense detects a greater number, it generates an alarm. |
| Data Frames Transmitted | Enter the maximum number of data frames per minute any Station is allowed to transmit. If AirDefense detects a greater number, it generates an alarm. |
| Data Frames Received | Enter the maximum number of data frames per minute any Station is allowed to receive. If AirDefense detects a greater number, it generates an alarm. |
| Mgmt Frames Transmitted | <p>Enter the maximum number of management frames per minute any Station is allowed to transmit. If AirDefense detects a greater number, it generates an alarm.</p> <p>Management frames carry information related to negotiating network connections. If many more Management frames per minute than usual are detected, this could indicate a Denial of Service attack, or that a hacker is flooding the air with "disassociate" or "de-authenticate" commands.</p> |
| Mgmt Frames Received | Enter the maximum number of management frames per minute any Station is allowed to receive. If AirDefense detects a greater number, it generates an alarm. |
| Ctrl Frames Transmitted | Enter the maximum number of control frames per minute any Station is allowed to transmit. If AirDefense detects a greater number, it generates an alarm. |
| Ctrl Frames Received | <p>Enter the maximum number of control frames per minute any Station is allowed to receive. If AirDefense detects a greater number, an alarm is generated.</p> <p>Control frames carry information about negotiating the 802.11 protocol for getting data onto the airwaves, and are transmitted at only 1 Mbs. Unusually high numbers of Control frames may indicate bandwidth and network problems.</p> |
| Fragment Frames Seen | Enter the maximum number of fragment frames per minute from any Station that are allowed. If AirDefense detects a greater number, it generates an alarm. |
| Decrypt Error Frames Seen | Enter the maximum number of decrypt error frames per minute from any Station that are allowed. If AirDefense detects a greater number, it generates an alarm. |

Access Point Thresholds

This set of thresholds applies to the Access Points themselves, and will typically be less than the Aggregate Station thresholds. These values should all be based on the "normal" WLAN traffic discovered your initial site survey. Entering a value of "0" (zero) for any threshold-type disables that specific alarm.

| Aggregate Station | Station | Access Point |
|---------------------------|-----------|--------------|
| Associations per Minute | 1 | |
| Bytes Transmitted | 9,000,000 | |
| Bytes Received | 9,000,000 | |
| Data Frames Transmitted | 900,000 | |
| Data Frames Received | 900,000 | |
| Mgmt Frames Transmitted | 2,000 | |
| Mgmt Frames Received | 2,000 | |
| Ctrl Frames Transmitted | 2,000 | |
| Ctrl Frames Received | 2,000 | |
| Fragment Frames Seen | 1 | |
| Decrypt Error Frames Seen | 1 | |

| Column | Description |
|-------------------------|---|
| Associations per Minute | Ordinarily, Access Points do not associate with anyone. However, when an Access Point is used as a "bridge" between two other parts of the wireless network, they must associate with the Access Points with whom they are bridging. Therefore this number should be "1" or the actual number of bridges in use. (If no bridges are deployed, this value should still be "1" as a zero value will disable alarm-generation for this threshold.) |
| Bytes Transmitted | Enter the maximum number of bytes of data per minute this Access Point is allowed to transmit. If AirDefense detects a greater number, it generates an alarm. |
| Bytes Received | Enter the maximum number of bytes of data per minute this Access Point is allowed to receive. If AirDefense detects a greater number, it generates an alarm. |
| Data Frames Transmitted | Enter the maximum number of data frames per minute this Access Point is allowed to transmit. If AirDefense detects a greater number, it generates an alarm. |
| Data Frames Received | Enter the maximum number of data frames per minute this Access Point is allowed to receive. If AirDefense detects a greater number, it generates an alarm. |
| Mgmt Frames Transmitted | Enter the maximum number of management frames per minute this Access Point is allowed to transmit. If AirDefense detects a greater number, it generates an alarm. |
| Mgmt Frames Received | Enter the maximum number of management frames per minute this Access Point is allowed to receive. If AirDefense detects a greater number, it generates an alarm. |

Steps to Use Create Policy: Vendor

- | Step | Action |
|------|--|
| 1 | Select the AirDefense (top) level of Tree View. |
| 2 | Click and pull down Create Policy: Vendor
<i>The Performance field appears.</i> |
| 3 | To edit an existing vendor policy, click Edit .
<i>You can click Reset at any time to get out of Edit mode without saving your changes.</i> |
| 4 | To add a custom vendor policy to the database, click Add (Add is disabled while in Edit mode).
<i>A Select Policies as Templates screen appears.</i>
<i>You can click Reset at any time to get out of Add mode without saving your changes.</i> |
| 5 | Select the default vendor you would like to form your custom vendor policy.
<i>A list of all known IEEE MAC prefixes for existing vendor equipment appears in the known prefixes field.</i>
<i>In the Policy Prefixes field, a list of existing prefixes appears. These are the prefixes that belong to the default vendor you selected.</i> |
| 6 | Use the right and left arrows to transfer prefixes back and forth between screens to form your custom vendor policy. |
| 7 | To permanently remove a performance policy from the database, click Delete (Delete is disabled while in Edit mode). |
| 8 | Click Commit to save your input. |

The table below lists the fields in the **Create Policy: Vendor** screen.

| Column | Description |
|--------------------------|--|
| Select Vendor Policy | This pick list displays all saved vendor policies. Once you formulate a custom vendor policy, it will appear on this list. You can select a policy from this list to edit or delete it. Included in the list is are Default policies—you cannot edit these.

<i>Note:</i> Default vendor policies are predefined and cannot be edited. Create a new vendor policy by using a default policy as a template. |
| Policy Name | This displays the name of the policy. |
| Description | This displays a description of the policy. |
| Applied to Access Points | This memo field displays all Access Points currently configured to use the currently selected policy. |
| MAC Prefixes | <ul style="list-style-type: none">• Known Prefixes: These are a list of all of the known IEEE MAC prefixes.• Policy Prefixes: These are list of the IEEE MAC prefixes that are vendor defaults, or the prefixes you assign in your custom vendor policy. |

5.5.4 Create Policy: Channel

Use the **Create Policy: Channel** fields to create channel policies for the Sensors in your WLAN. AirDefense allows you to set ad hoc networking and time-of-day policies for individual channels. Whenever one of AirDefense's Sensors detects an ad hoc network or network traffic outside of allowed hours, it generates an alarm.

You can navigate to this screen by:

- Using the screen pull-down **Create Policy: Channel**
- Clicking on any Sensor in Tree View, and then clicking on **Channel Policy: Policy Editor**.
- Clicking on **Apply Policy: Sensor** (with **Set Channel Policy** selected)

Policy Manager - Channel Policy
Last updated: Tue Jan 14 10:29:41 EST 2003

Navigation: [Back] [Forward] [Cancel] [Apply] [Add] [Delete] [Reset]

Tree View:

- Your Company Name
 - Default Location
 - Default Group
 - Default Sensor
 - Added Access Points
 - 00:02:2d:3f:25:60
 - 00:06:24:54:99:61
 - 00:07:50:ca:14:18
 - Added Stations
 - 00:02:2d:3f:25:6a
 - 00:00:00:00:00:00
 - 00:00:00:00:00:00
 - New York
 - Queens
 - 6E1F-77

Select Channel Policy: [Default]

Policy Name: Default

Description: This is the default channel policy that will be applied to all sensors when they are first discovered.

Applied to Sensors: 00:00:00:00:00:00, 00:00:00:00:00:00, 00:00:00:00:00:00

| Channel | Allow Ad Hoc | Valid Activity Hours |
|------------|---|-----------------------------------|
| Channel 1 | <input checked="" type="radio"/> Yes <input type="radio"/> No | Start Time: 12:00 End Time: 14:00 |
| Channel 2 | <input type="radio"/> Yes <input checked="" type="radio"/> No | Start Time: 00:00 End Time: 00:00 |
| Channel 3 | <input type="radio"/> Yes <input checked="" type="radio"/> No | Start Time: 00:00 End Time: 00:00 |
| Channel 4 | <input type="radio"/> Yes <input checked="" type="radio"/> No | Start Time: 00:00 End Time: 00:00 |
| Channel 5 | <input type="radio"/> Yes <input checked="" type="radio"/> No | Start Time: 00:00 End Time: 00:00 |
| Channel 6 | <input type="radio"/> Yes <input checked="" type="radio"/> No | Start Time: 00:00 End Time: 00:00 |
| Channel 7 | <input type="radio"/> Yes <input checked="" type="radio"/> No | Start Time: 00:00 End Time: 00:00 |
| Channel 8 | <input type="radio"/> Yes <input checked="" type="radio"/> No | Start Time: 00:00 End Time: 00:00 |
| Channel 9 | <input type="radio"/> Yes <input checked="" type="radio"/> No | Start Time: 00:00 End Time: 00:00 |
| Channel 10 | <input type="radio"/> Yes <input checked="" type="radio"/> No | Start Time: 00:00 End Time: 00:00 |
| Channel 11 | <input type="radio"/> Yes <input checked="" type="radio"/> No | Start Time: 00:00 End Time: 00:00 |
| Channel 12 | <input type="radio"/> Yes <input checked="" type="radio"/> No | Start Time: 00:00 End Time: 00:00 |
| Channel 13 | <input type="radio"/> Yes <input checked="" type="radio"/> No | Start Time: 00:00 End Time: 00:00 |
| Channel 14 | <input type="radio"/> Yes <input checked="" type="radio"/> No | Start Time: 00:00 End Time: 00:00 |

Steps to Use Create Policy: Channel

- | Step | Action |
|------|--|
| 1 | Select the AirDefense (top) level of Tree View. |
| 2 | Click and pull down Create Policy: Channel
<i>The Channel field appears.</i> |
| 3 | To edit an existing channel policy, click Edit . |

*You can click **Reset** at any time to get out of Edit mode without saving your changes.*

- 4 To add a custom channel policy to the database, click **Add** (Add is disabled while in Edit mode).
*You can click **Reset** at any time to get out of Add mode without saving your changes.*
- 5 Enter the policy name.
- 6 Enter the policy description.
- 7 Configure channels 1-14 with Allow Ad Hoc (yes/no) and valid activity hours (Start Time/End Time).
- 8 Click **Commit** to save your input.

The table below lists the top fields in the in the **Create Policy: Channel** screen.

| Field | Purpose |
|--------------------------|---|
| Select Channel Policy | This pick list displays all saved channel policies. Select a policy from this list, or you can click Add to edit your existing custom policy, or design a new policy. You can click Delete to remove channel policies. Included in the pick list is a Default policy (cannot be edited). |
| Policy Name | This displays the name of the policy. |
| Description | This displays a description of the policy. |
| Applied to Access Points | This memo field displays all Access Points currently configured to use the currently selected policy. |
| Channel Configurations | <p>Channel Number: You must make configurations for each of the 14 channels.</p> <p>Allow Ad Hoc: Choose Yes to allow Ad Hoc; No to disallow Ad Hoc. Ad Hoc is independent of activity hours.</p> <p><i>Note:</i> An ad hoc station is a User Station that is connected to one or more other User Stations without using an Access Point. Although ad hoc networking is a function of most standard 802.11 network client cards, User Stations that are connected in this manner do not need a wireless infrastructure, and therefore represent a security threat, especially when one or more User Stations in the ad hoc network also connect to a wired network.</p> <p>Valid Activity Hours: For each channel, enter a Start Time and End Time in the input fields.</p> <p><i>Note:</i> Enter times in a 24-hour format, using the format HH:MM. Traffic is <i>only</i> allowed between the start and end hours. Traffic detected on the channel outside this window generates an alarm.</p> |



Creating a No-Use Time-of-Day Channel Policy

To create an effective “no-use” time-of-day policy for a channel, enter a Start Time and End Time that are only one minute apart, e.g., 01:00 and 01:01. Entering 00:00 in *both* the Start Time and End Time *disables* alarm-generation for that channel.

Also, you may wish to explicitly set time-of-day and ad hoc policies for channels you know are not supposed to be in use. Even if you don’t have a Sensor dedicated to scanning *all* channels, your deployed Sensors—even if locked onto just one channel—will hear network traffic bleeding over from adjacent channels, and will generate alarms based on them. This may assist you in tracking down unauthorized wireless users.

5.6 Apply Policy

To apply the policies you created in Create Policies, you must access four program areas. These are:

- Global
- Sensor
- Access Point
- Station

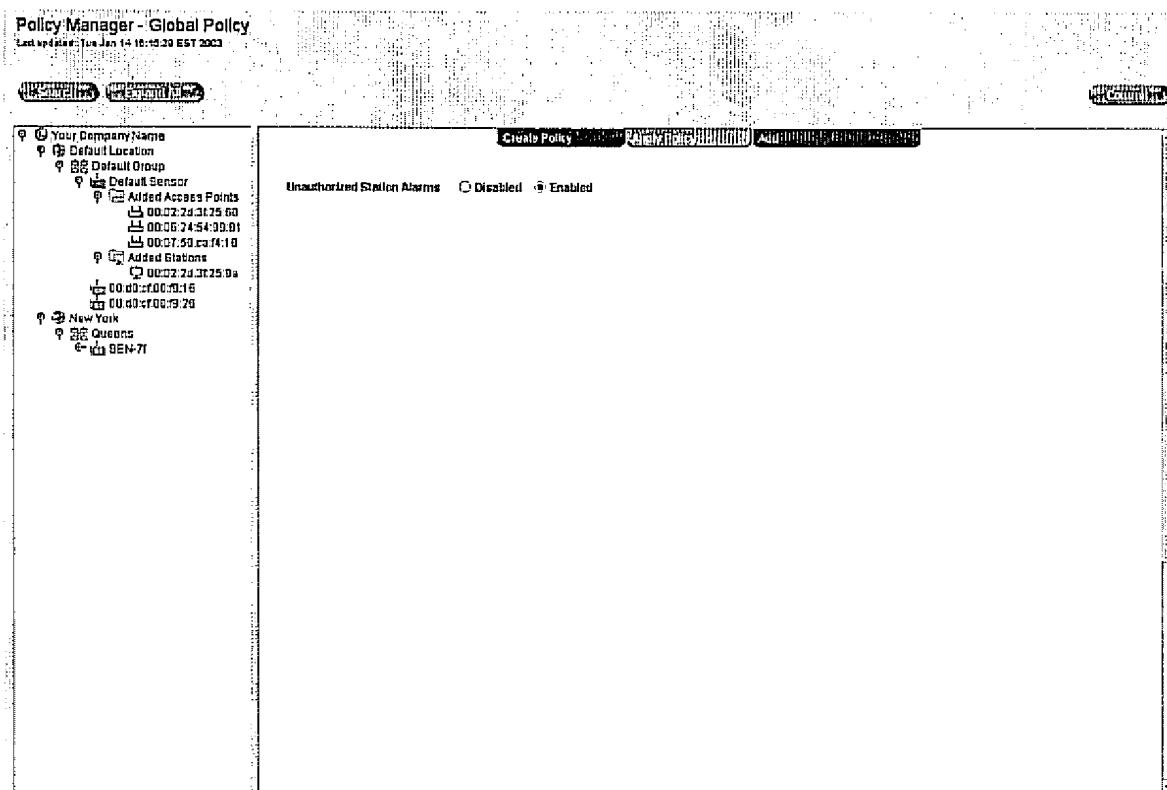
5.6.1 Apply Policy: Global

Use the **Apply Policy: Global** screen to disable or enable unauthorized Station alarms your WLAN.

Note: Unauthorized Station alarms are generated for Stations that are associated with an authorized Access Point, but are not on that Access Point's list of valid Stations.

You can navigate to this screen by:

- Using the screen pull-down **Apply Policy: Global**



Steps to Use Apply Policy: Global

- | Step | Action |
|------|--|
| 1 | Select the AirDefense (top) level of Tree View. |
| 2 | Click and pull down Apply Policy: Global
<i>The Global Policy fields appears. The field has two selections: Enabled or Disabled.</i> |
| 3 | Click Enable to enable all unauthorized station alarms, or Disable to disable all unauthorized Station alarms in your WLAN. |
| 4 | Click Commit . |

The table below lists the fields in the **Apply Policy: Global** screen.

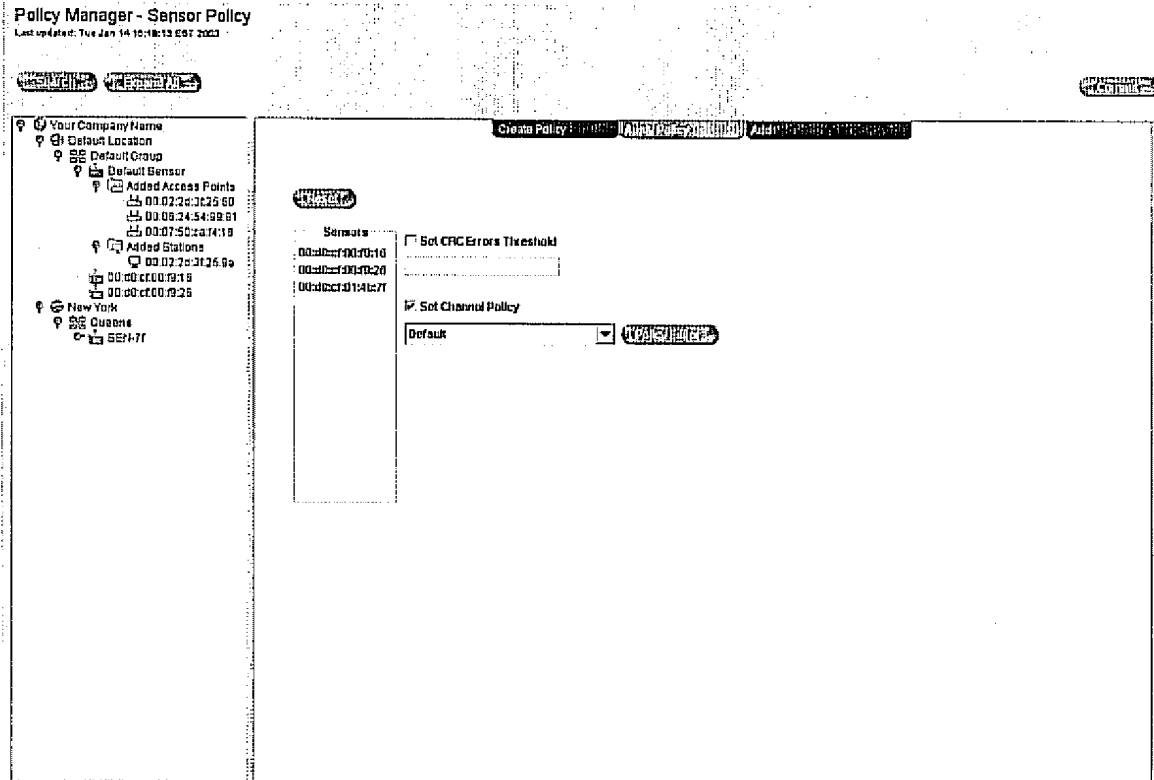
| Field | Purpose |
|-----------------------------|---|
| Unauthorized Station Alarms | <ul style="list-style-type: none">• Disabled: Click disable and the AirDefense Server will not generate an alarm if it detects an unauthorized Station.• Enabled: Click Enable and the AirDefense Server will generate an alarm whenever it detects an unauthorized Stations in the portion of the WLAN the Sensor is monitoring. |

5.6.2 Apply Policy: Sensor

Use **Apply Policy: Sensor** to apply your policies to the Sensors in your WLAN.

You can navigate to this screen by:

- Using the screen pull-down **Apply Policy: Sensor**



Steps to Use Apply Policy: Sensor

- | Step | Action |
|------|---|
| 1 | Select the AirDefense (top) level of Tree View. |
| 2 | Click and pull down Apply Policy: Sensor |

The Sensor Policy screen appears. This screen has three subscreens: A color-coded list of Sensors in your WLAN; Set CRC Errors Threshold; and Set Channel Policy.

Note: Clicking on the Policy Editor button takes you to the Channel Policy Editor (**Create Policy: Channel** screen).



*You can click **Reset** at any time to get out of Edit mode without saving your changes.*

- | | |
|---|---|
| 3 | Click on the CRC Errors Threshold checkbox to enable the field, and enter the required information. |
| 4 | Click on the Set Channel Policy checkbox to enable the field, and enter the required information. |
| 5 | Click Commit . |

The table below lists the fields in the Apply Policy: Sensor screen.

| Field | Purpose |
|--------------------------|--|
| Sensors | This is a list of observed Sensors in your WLAN. The Sensor is color coded (see "Color Codes" on page 83). |
| Set CRC Errors Threshold | <p>This is the threshold for the number of CRC errors allowed in WLAN the Sensor is monitoring.</p> <p>Enter a number of CRC errors per minute each Sensor may detect as it listens to the traffic in its reception area. High numbers of CRC errors may indicate that two or more Access Points are sharing the same channel; colliding with each other; that an object is interfering with the signal; or that a hacker may be flooding your air space with bad data in a Denial of Service attempt.</p> <p><i>Note:</i> Unusually high numbers of CRC errors indicate network performance problems or the activity of a hacker.</p> |
| Set Channel Policy | <p>This pick list displays all saved channel policies. Select a policy from this list to apply to each Sensor in the Sensors list. Alternately, you can click Policy Editor to go to the Channel Policy Editor screen and edit, add, or delete channel policies.</p> <p><i>Note:</i> Default policies cannot be edited.</p> |

5.6.3 Apply Policy: Access Point

Use **Apply Policy: Access Point** to apply your policies to one or more Access Points in your WLAN.

You can navigate to this screen by:

- Using the screen pull-down **Apply Policy: Access Point**

Steps to Use Apply Policy: Access Point

| Step | Action |
|------|---|
| 1 | Select the AirDefense (top) level of Tree View. |
| 2 | Click and pull down Apply Policy: Access Point |
| 3 | Select an Access Point to apply your policies to. |
| 4 | Click Commit . |

The Access Point Policy fields appear. The main screen shows all Access Points in your WLAN.

You can select configuration, performance, and vendor policies by clicking on the associated checkbox. Clicking Policy Editor takes you to the Configuration, Performance, and Vendor Policy Editing screens, where you can edit, add, and delete policies.

*You can click **Reset** at any time to get out of Edit mode without saving your changes.*

The table below lists the fields in the **Apply Policy: Access Point** screen.

| Field | Purpose |
|--------------------------------|---|
| Access Points | This is a list of observed Access Points in your WLAN.

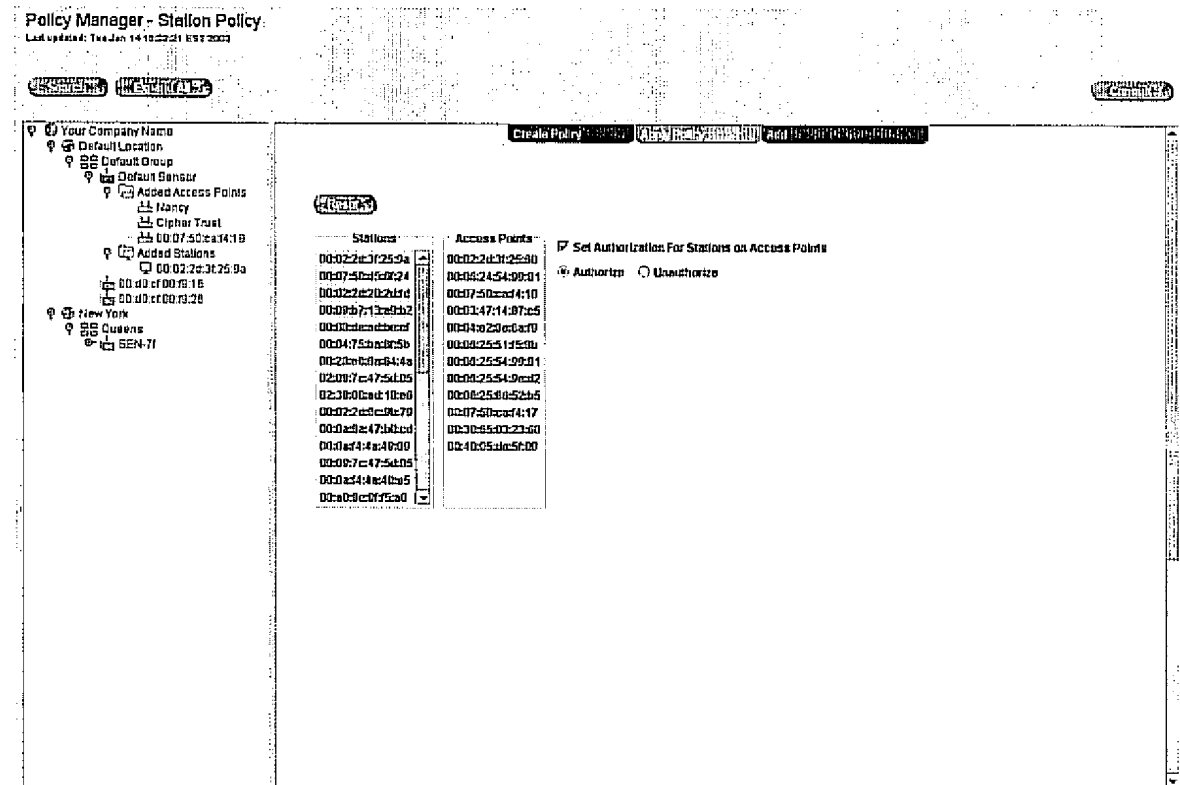
<i>Note:</i> Holding the mouse over an Access Point icon brings up a rollover screen that shows its Device Identifier. |
| Set Access Point Authorization | <ul style="list-style-type: none"> • Authorize: Select Authorize if this Access Point is a legitimate Access Point in your WLAN. • Unauthorize: Select Unauthorize if this Access Point is not legitimate. If it is not authorized here, the AirDefense Server will generate an alarm once a minute whenever that Access Point is detected by a Sensor. (All detected Access Points <i>not authorized</i> are assumed to belong to hackers or violators of your wireless network policy.) |
| Set Configuration Policy | Clicking the checkbox allows you to select a default or custom configuration policy to apply to an Access Point. You can also click Policy Editor to go to the Configuration Policy Editor screen, where you can edit, add, or delete configuration policies. |
| Set Performance Policy | Clicking the checkbox allows you to select a default or custom performance policy for an Access Point. You can also click Policy Editor to go to the Performance Policy Editor screen, where you can edit, add, or delete performance policies. |
| Set Vendor Policy | Clicking the checkbox allows you to select a default or custom vendor policy for an Access Point. You can also click Policy Editor to go to the Vendor Policy Editor screen, where you can edit, add, or delete performance policies. |

564 Apply Policy: Station

Use Apply Policy: Station to authorize or unauthorize Stations on Access Points in your WLAN. This feature allows you to authorize one Station on multiple Access Points. This useful feature allows you to authorize one user in the WLAN to use the network from multiple physical locations.

You can navigate to this screen by:

- Using the screen pull-down **Apply Policy: Station**



Steps to Use Apply Policy: Station

| Step | Action |
|------|--|
| 1 | Select the AirDefense (top) level of Tree View. |
| 2 | Click and pull down Apply Policy: Station |

The Station Policy fields appear. The screen has three subscreens: An icon and color-coded list of Stations in your WLAN; an icon and color-coded list of Access Points your WLAN; and a field to authorize or de-authorize Stations on Access Points.

- 3 Select a Station and the Access Point you wish to authorize or unauthorize.
- 4 Click the checkbox to open the field.
 - Select **Authorize** to authorize a Station on an Access Point.
 - Select **Unauthorize** to unauthorize a Station on an Access Point.

You can click **Reset** at any time to get out of Edit mode without saving your changes.

- 5** Click **Commit**.

The table below lists the fields on the **Apply Policy: Station** screen.

| Field | Purpose |
|---|---|
| Stations | <p>This is a list of observed Stations in your WLAN. The Stations are icon and color coded (see "Color Codes" on page 83).</p> <p><i>Note:</i> Holding the mouse over an Access Point icon brings up a rollover screen that shows its Device Identifier.</p> |
| Access Points | <p>This is a list of observed Access Points in your WLAN. The Access Points are icon and color coded (see "Color Codes" on page 83).</p> <p><i>Note:</i> Holding the mouse over an Access Point icon brings up a rollover screen that shows its Device Identifier.</p> |
| Set Authorization for Stations on Access Points | <ul style="list-style-type: none"> You must click on the checkbox before selecting authorize/unauthorize. Authorize: Select Authorize if this Station is a legitimate Station assigned to an legitimate Access Point in your WLAN. Unauthorize: Select Unauthorize if this Station is not legitimate. If it is not authorized here, the AirDefense Server will generate an alarm once a minute whenever a Sensor detects the Station. (All detected Stations <i>not authorized</i> are assumed to belong to hackers or violators of your wireless network policy.) |

The Add/Import function of Policy Manager enables you to pre-configure and add Access Points and Stations to your WLAN manually, or by importing from a list of Access Points or Stations contained on a flat file. You can also use the Add/Import function to import user information.

Using **Policy Manager: Add/Import** will enable you to add Access Points and Stations to your WLAN that are already configured for authorization; configuration, performance, and vendor policies; and other operational behaviors.

You can use **Policy Manager: Add/Import** to:

- Pre-configure Access Points before adding them to your WLAN. This includes configuring the Access Point for authorized, unauthorize, or ignore; determining whether or not the Access Point is a bridge; and assigning or editing policies for the Access Point.
- Pre-configure Stations before adding them to your WLAN. This includes configuring the Station for a LEAP Username assignment (if applicable); placing the Station on a Watch or Ignore List; and authorizing or unauthorizing the Station for an Access Point.
- Import Access Points and Station MAC addresses from an ASCII comma-delimited flat file, and configure all of them prior to adding them to your WLAN.

Add has five screens. These are:

- Access Point
- Station
- Import Access Points
- Import Stations
- Import ACS Config

6.7.1 Add Access Point

Use the **Add: Access Point** screen to manually pre-configure and add an Access Point to your WLAN.

You can navigate to this screen by:

- Using the screen pull-down **Add: Access Point**

Policy Manager - AP View
Last updated: Tue Jan 14 15:20:28 EST 2003

Commit

Tree View:

- Your Company Name
 - Default Location
 - Default Group
 - Default Sensor
 - Add: Access Point**
 - Nancy
 - Cipher Trust
 - 00:07:50:ca:74:10
 - Add: Access Point**
 - 00:02:2d:2f:25:9a
 - 00:00:00:00:00:00
 - 00:00:00:00:00:00
 - New York
 - Queens
 - SE4-11

Form Fields:




 - Access Point ID:
 - Access Point Name:
 - Description:
 - Service Set ID:
 - Access Point Vendor:
 - IP Address:
 - DNS Name:
 - Bridge: ☐ Yes ☐ No
 - Authorized Access Point: ☐ Yes ☐ No ☐ Custom
 - Configuration Policy: ☐ **Policy Editor**
 - Performance Policy: ☐ **Policy Editor**
 - Vendor Policy: ☐ **Policy Editor**

Commit

Steps to Use Add: Access Point

- | Step | Action |
|------|---|
| 1 | Select the AirDefense (top) level of Tree View. |
| 2 | Click and pull down Add: Access Point
<i>The Add Access Point screen appears.</i> |
| 3 | Enter information into the open fields (see the table that follows for an explanation of each field).
<i>You can select configuration, performance, and vendor policies by clicking on the associated checkbox. Clicking Policy Editor takes you to the Configuration, Performance, and Vendor Policy Editing screens, where you can edit, add, and delete policies.</i> |
| 4 | Click Commit . |

The table below lists the fields in the Add: Access Point screen.

| Field | Purpose |
|-------------------------|--|
| Access Point ID | MAC address of the Access Point. This is a required field. |
| Name | Name of the Access Point (optional) |
| Description | A description of the Access Point (optional) |
| Service Set ID | SSID number (this is not the same as the Access Point ID). |
| Access Point Vendor | Equipment manufacturer of the Access Point. |
| IP Address | The IP address of the Access Point. |
| DNS Name | The Access Point's DNS Name assignment (if applicable). |
| Bridge | <ul style="list-style-type: none"> Yes: Click Yes if you are using this Access Point as a Bridge No: Click No if you are not using this Access Point as a Bridge |
| Authorized Access Point | <ul style="list-style-type: none"> Yes: Click Yes to authorize this Access Point for use in your WLAN No: Click No to unauthorize this Access Point for use in your WLAN Ignore: Click Ignore to place this Access Point in an Ignored state. <p><i>Note:</i> This feature is useful if you want to keep certain unauthorized Access Points or Stations your AirDefense Server sees from alarming, and thus preventing continuous false alarms. Sensors can detect Access Points in neighboring WLAN systems. When this happens, AirDefense generates an alarm. Designating an Access Point as Ignored prevents the Access Point and all Stations associated with the Access Point from alarming. If an attack occurs, an alarm generates regardless.</p> |
| Configuration Policy | <p>Leaving the default configuration policy for the Access Point in place, or specify a custom policy.</p> <p>Click Policy Editor to go to the Configuration Policy Editor screen if you wish to edit, add, or delete configuration policies.</p>  |
| Performance Policy | <p>Leaving the default performance policy for the Access Point in place, or specify a custom policy.</p> <p>Click Policy Editor to go to the Performance Policy Editor screen if you wish to edit, add, or delete performance policies.</p>  |
| Vendor Policy | <p>Leaving the default vendor policy for the Access Point in place, or specify a custom policy.</p> <p>Click Policy Editor to go to the Vendor Policy Editor screen if you wish to edit, add, or delete vendor policies.</p>  |

5.7.2 Add Station

Use the **Add: Station** screen to manually pre-configure and add a Station to your WLAN.

You can navigate to this screen by:

- Using the screen pull-down **Add: Station**

Policy Manager - Add Station
Last updated: Tue Jan 14 15:25:41 EST 2003

CSM/MSM **WLAN**

Create Policy **Apply Policy** **Cancel** **Commit**

Your Company Name
Default Location
Default Group
Default Sensor
Unassociated Stations
East Side
South Side
West Side

Station ID
Station Name
Description
LEAP Username
Vendor Name
IP Address
DNS Name
List Options ☐ Watch List ☐ Ignore List
Access Points ☐ Set Access Control List ☐ Show in all access points
☐ Authenticate ☐ Unauthenticated

Steps to Use Add: Station

- | Step | Action |
|------|---|
| 1 | Select the AirDefense (top) level of Tree View. |
| 2 | Click and pull down Add: Station
<i>The Add Station screen appears.</i> |
| 3 | Enter information into the open fields (see the table that follows for an explanation of each field). |
| 4 | Click Commit . |

Add Station displays the following.

| Field | Displays... |
|--|--|
| Station ID | The MAC address of the Station. AirDefense automatically generates this field. |
| Name | The Name of the Station (optional) |
| Description | A description of the Station (optional) |
| LEAP Username | The LEAP Username. This field applies if you are using EAP Configuration Mode in your configuration policy definition. (See "Create Policy: Configuration" on page 99.) |
| Vendor Name | The equipment manufacturer of the Station. AirDefense automatically generates this field. |
| IP Address | The IP address of the Station. |
| DNS Name | The Station's DNS Name assignment (if applicable). |
| List Options | <p>If you are going to use a List Option, the option must be either Watch List, or Ignore.</p> <ul style="list-style-type: none"> • Watch List: Click on this checkbox if you wish to know if this Station's MAC address will occur in your network again. The next time the AirDefense Server sees this Station, it will generate an alarm for every minute the it sees this Station's in the network. The Watch list is unrelated to authorized/unauthorized states. • Ignore List: Click on this checkbox if you wish the AirDefense Server to ignore the presence of a Station on the network. AirDefense does not generate an alarm for any devices on the Ignore list. <p><i>Note:</i> This feature is useful if you want to keep certain unauthorized Stations that your AirDefense Server sees from alarming, as in the case of Stations in an adjacent office that belong to another Company. Placing these known "friendly" Stations on the Ignore list prevents continuous false alarms.</p> |
| Access Points | List of Access Points that the Station is associated with. |
| Set Authorization For Station on Access Points | <ul style="list-style-type: none"> • You must click on the checkbox before selecting authorize/unauthorize. • Authorize: Select Authorize if this Station is a legitimate Station assigned to an legitimate Access Point in your WLAN. • Unauthorize: Select Unauthorize if this Station is not legitimate. If it is not authorized here, the AirDefense Server will generate an alarm once a minute whenever a Sensor detects the Station. (All detected Stations <i>not authorized</i> are assumed to belong to hackers or violators of your wireless network policy.) |

573 Add: Import Access Points

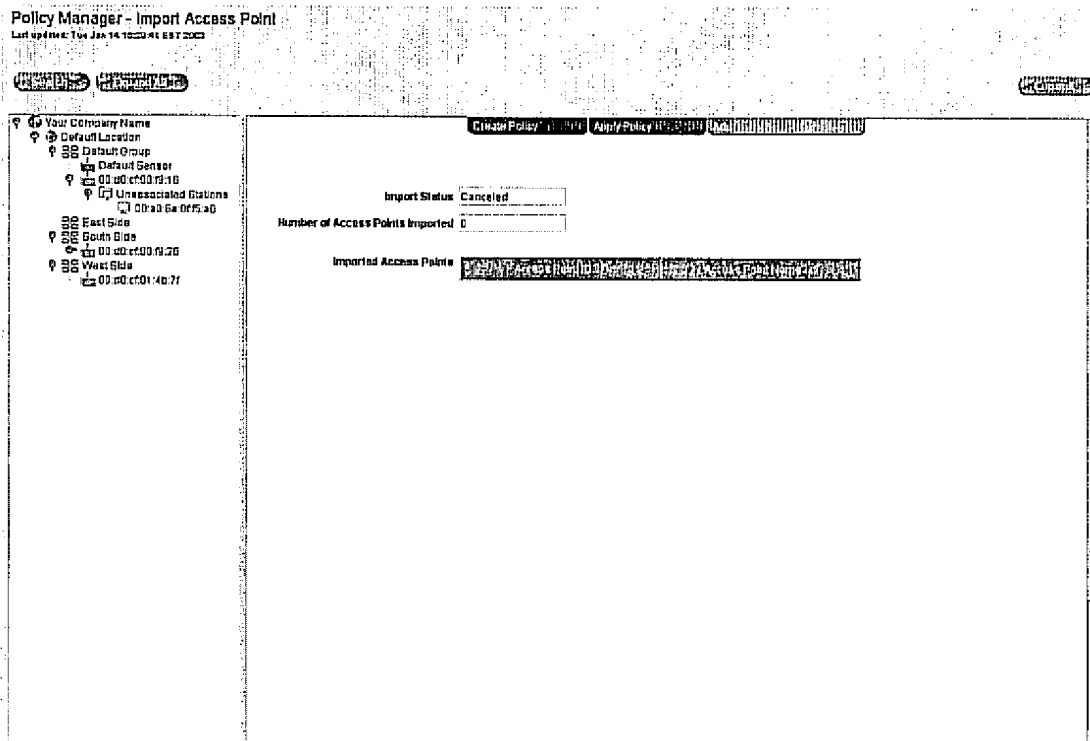
Use the **Add: Import Access Points** screen to import an Access Points into your WLAN.

Note: When you import an Access Point that has never been seen by AirDefense, it will appear as Blue (unassociated) in Tree View. Once AirDefense sees the Access Point, the Access Point will become Green (if you authorized it prior to import), or Red (if you did not authorize it prior to import). The Access Point will move to an associated location in the tree.

Important: AirDefense rejects any file that is not in the correct format or if you have exceeded your license agreement count. See Appendix B: File Import Formats for the correct file format. See Chapter 8, Administration, on page 217 for information regarding license agreements.

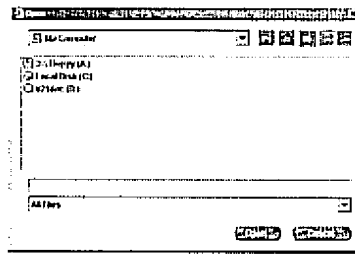
You can navigate to this screen by:

- Using the screen pull-down **Add: Import Access Points**



Steps to Use Add: Import Access Points

- | Step | Action |
|------|--|
| 1 | Select the AirDefense (top) level of Tree View. |
| 2 | Click and pull down Add: Import Access Points
<i>A browser window appear</i> |



- 3 Navigate to the desired file, and select the file.
- 4 Click **Commit**.

Import Access Points displays the following:

| Field | Displays... |
|----------------------------------|---|
| Import Status | The status of the current import. |
| Number of Access Points Imported | The number of Access Points being imported into AirDefense. |
| Imported Access Points | Access Point ID: The Device Identifier of the Access Point.
Access Point Name: The user-configured name of the Access Point. |

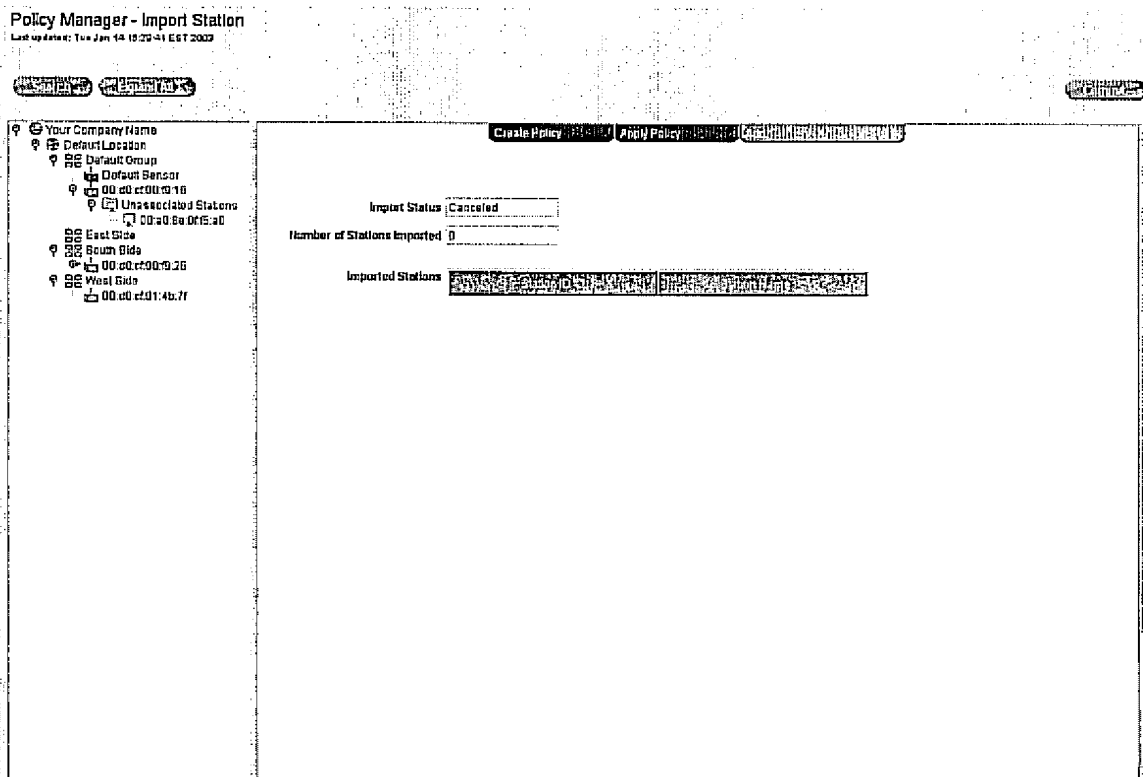
574 Add: Import Stations

Use the **Add: Import Stations** screen to import a list of Stations into your WLAN.

Important: When you import a station, it overwrites all information that is already in AirDefense. AirDefense rejects any file that is not in the correct format. See Appendix B: File Import Formats for the correct file format.

You can navigate to this screen by:

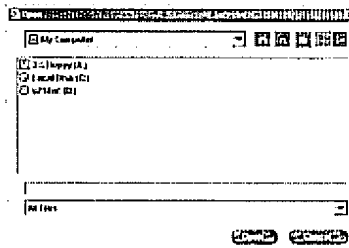
- Using the screen pull-down **Add: Import Stations**



Steps to Use Add: Import Stations

To use the **Add: Import Stations** screen, do the following:

| Step | Action |
|------|---|
| 1 | Select the AirDefense (top) level of Tree View. |
| 2 | Click and pull down Add: Import Stations
<i>A browser window appears.</i> |



- 3 Navigate to the desired file, and select the file.
- 4 Click **Commit**.

Import Stations displays the following:

| Field | Displays... |
|-----------------------------|---|
| Import Status | The status of the current import. |
| Number of Stations Imported | The number of Stations being imported into AirDefense. |
| Imported Stations | Access Point ID: The Device Identifier of the Station.
Access Point Name: The user-configured name of the Station. |

5.7.5 Import ACS Config

Use **Add: Import ACS Config** to import Access Points and Stations into AirDefense from a Cisco Access Control Server.

The screenshot displays the 'Policy Manager - Import External Config' window. The left sidebar shows a tree view of configuration elements under 'AirCommand', including 'Default Location', 'Default Group', 'Default Sensor', 'Linksys net', 'default', 'Unassociated Stations', 'Linksys', 'QA Link', 'Unknown_SSID', 'EMX AirPort', and 'QAVLAN 350'. The main panel shows the 'Import ACS Config' process with the following details:

- Import Status:** Complete
- Number of APs Imported:** 2
- Imported APs:**

| Access Point ID | Access Point Name | Status |
|-------------------|-------------------|----------|
| 00:00:00:00:00:00 | 10.5.0.2 | Approved |
| 00:07:50:ca:14:17 | | Approved |
- Number of Stations Imported:** 1
- Imported Stations:**

| Access Point ID | Access Point Name | Status |
|-------------------|-------------------|----------|
| 00:06:43:74:50:35 | | Approved |

Prerequisites to Use Add: Import ACS Config

To use Add: Import ACS Config, you must have downloaded two.txt files into your workstation. These files are:

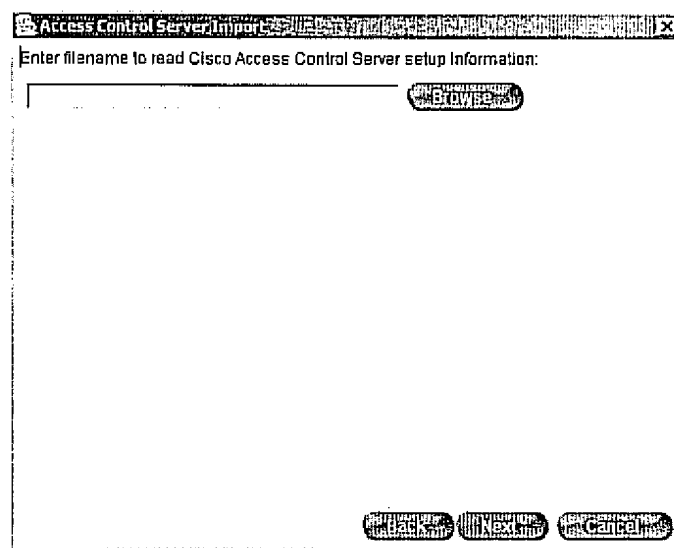
- Import Access Control Server **Setup** File
- Access Control Server **Dump** File

You can get these files from Cisco, from the server that is running ACS, using their command line tool.

Steps to Use Add: Import ACS Config

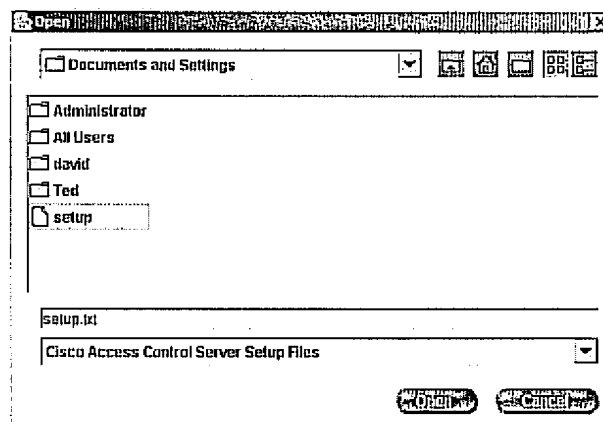
- | Step | Action |
|------|---|
| 1 | Select the AirDefense (top) level of Tree View. |
| 2 | Click and pull down Add: Import ACS Config . |

The following window appears.



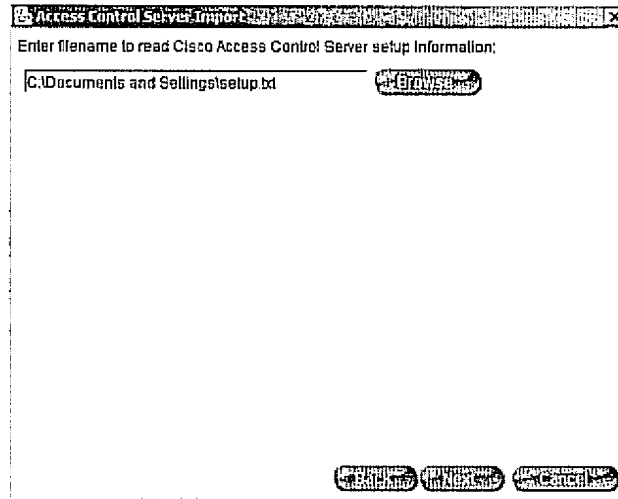
- 3 Find the data.txt file. Click Browse to find the file in your database directory.

A Browser window appears.



- 4 Select the **Setup.txt** file and click **Open**.

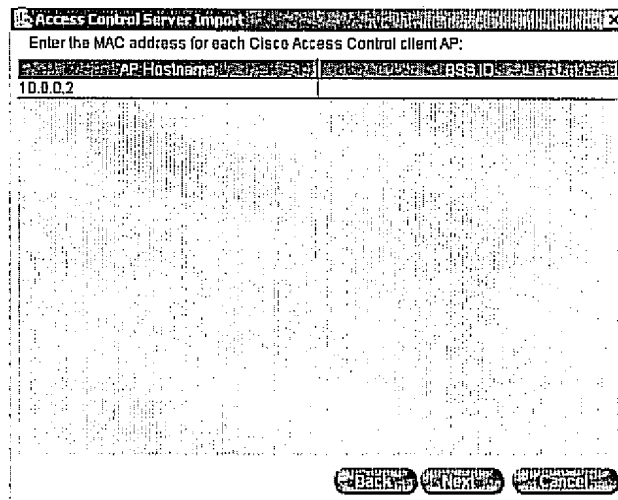
The following window appears, showing the path with Setup.txt file.



- 5 Click **Next**.

This reads the setup file, which contains the Hostname and other information about the Cisco Access Control Access Point—the Access Point that directly connects to the Cisco Control Server. This is an authentication step.

The following window appears.

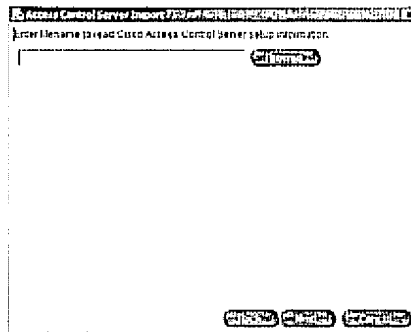


- 6 Double-click in BSS ID column. In this column, enter the MAC address of each Access Point Hostname that appears.

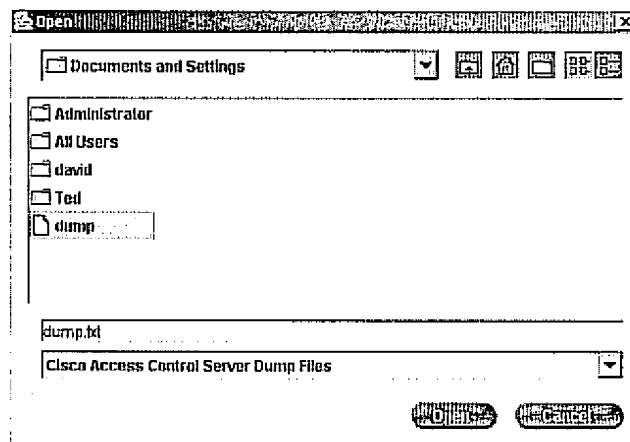
Note: If you do not enter a valid MAC address for each Access Point, you cannot proceed.

- 7 Click **Next**.

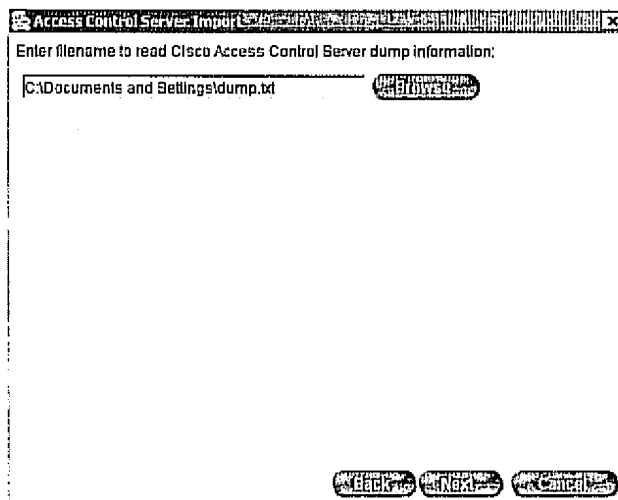
The following window appears



- 8 Find the dump.txt file. Click Browse to find the file in your database directory.
A Browser window appears.



- 9 Select the **Dump.txt** file and click **Open**.
The path with Dump.txt file appears in the Access Control Server Import window.



10 Click **Next**.

The following window appears, which lists Access Points and Stations to be imported.

Access Control Server Import

Verify data from Access Control Import and press Done:

APs to be imported:

| AP ID | AP Name | AP Status |
|-------------------|----------|---------------|
| 00:00:00:00:00:00 | 10.0.0.2 | Not Available |
| 00:07:50:ca:74:17 | | Not Available |

Stations to be imported:

| Station ID | Station Name | Station Status |
|-------------------|--------------|----------------|
| 00:09:43:74:50:35 | | Not Available |

Buttons:

11 Click **Done**.

Alternately, you can click **Cancel** to leave the window with no changes.

The Import External Config screen appears, with fields populated.

Policy Manager - Import External Config
Last updated: Feb 24 17 10:27:14 EST 2003

Buttons:

Left Panel (Tree View):

- AirCommand
 - Default Location
 - Default Group
 - Default Sensor
 - Linksys net
 - 00:00:25:54:00:02
 - 00:00:00:00:00:00
 - 00:07:50:ca:74:17
 - 00:09:43:74:50:35
 - 00:00:00:00:00:00
 - 00:00:00:00:00:00

Main Panel:

Buttons:

Import Status: Complete

Number of APs Imported: 2

| AP ID | AP Name | AP Status |
|-------------------|----------|-----------|
| 00:00:00:00:00:00 | 10.0.0.2 | Approved |
| 00:07:50:ca:74:17 | | Approved |

Number of Stations Imported: 1

| Station ID | Station Name | Station Status |
|-------------------|--------------|----------------|
| 00:09:43:74:50:35 | | Approved |

Imported Stations:

12 Click **Commit** to save all changes.

Import ACS Config. displays the following:

| Field | Displays... |
|-----------------------------|---|
| Import Status | The status of the current import. <ul style="list-style-type: none">• Pending: Import is in process• Cancelled: Import was cancelled• Complete: Import is complete |
| Number of APs Imported | The number of Access Points being Imported into AirDefense. |
| Imported APs | Information on the imported Access Points. <ul style="list-style-type: none">• BSS ID: The MAC address of the Access Point.• AP Host Name: The user-configured name of the Access Point. This depends on what is entered into the Cisco server. For Access Points, this is usually the IP address.• Status: Information on licensing.<ul style="list-style-type: none">— Not available: Licensing not available for Access Points being imported— Approved: Licensing approved for Access Points being imported— Denied: License exceeded |
| Number of Stations Imported | The number of Stations being imported into AirDefense. |
| Imported Stations | Information on the imported Stations. <ul style="list-style-type: none">• Station ID: The Device Identifier of the Station.• Station Name: The user-configured name of the Station• Status: Information on licensing.<ul style="list-style-type: none">— Not available: Licensing not available for Stations being imported— Approved: Licensing approved for Stations being imported— Denied: License exceeded |